JEFFREY B. COOPERSMITH (SBN 252819)
AMY WALSH (Admitted *Pro Hac Vice*)
STEPHEN A. CAZARES (SBN 201864)
ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105-2669
Telephone: (415) 773-5700
Facsimile: (415) 773-5759

Email: jcoopersmith@orrick.com; awalsh@orrick.com;
scazares@orrick.com

Attorneys for Defendant
RAMESH "SUNNY" BALWANI

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. RAMESH "SUNNY" BALWANI, Defendant.	Case No. CR-18-00258-EJD **DECLARATION OF RICHARD L. SONNIER III** Hon. Edward J. Davila

DECLARATION OF RICHARD L. SONNIER III

I, Richard L. Sonnier III, declare as follows:

1. I have been retained by Defendant Ramesh "Sunny" Balwani to serve as an expert in the field of Microsoft SQL databases and attendant equipment and software, including encryption of such databases and recovery of data from them.

2. My services are being billed at an hourly rate of $300 per hour. I am being separately reimbursed for any out-of-pocket expenses. My compensation in no way depends on the outcome of this investigation or the particular testimony or opinions that I express.

I. BACKGROUND & EXPERIENCE

3. My qualifications as an expert witness can be found in Exhibit A, which includes my CV and a list of my publications and previous testimony.

II. SUMMARY AND SCOPE OF OPINIONS

4. After reviewing materials on Theranos's Laboratory Information System ("LIS"), I have determined that the government's claim that it could have done nothing to access the LIS and extract data from it without a lost encryption key is incorrect. The government could have accessed the LIS to obtain data from it either before or after Theranos disassembled the system at the end of August 2018, when I understand the company was winding down. The technical procedures that the government could have used to acquire or recover LIS data include obtaining possession of the equipment running the LIS database either before or long after August 31, 2018, or obtaining possession of the disk drives for the LIS system before or long after August 31, 2018. The government would ***not*** have needed the missing password for the private encryption key if it had used these procedures, as discussed below.

III. MATERIALS CONSIDERED

5. In forming the opinions expressed in this report, I considered and relied on my education, experience, and knowledge of the relevant fields. I also reviewed and considered the materials listed in Exhibit B.

6. I reserve the right to rely on any other information, deposition testimony, trial testimony, documents, or materials that may be provided to me or that witnesses at trial rely on if called to testify about any aspect of this matter.

IV. THE LIS DATABASE AND LIS SYSTEM

7. As a starting point, LIS consists of the LIS database and the LIS system. The LIS database is the heart of the LIS system where all the laboratory data is stored. My review of the materials shows that the LIS database was contained in at least 11 Microsoft SQL Server databases.[1] The LIS system, on the other hand, consisted of the LIS database and also the software that provided functionality, such as inputting and recording patient lab results, quality control results, and customer and physician interaction data. The LIS system also had features that allowed for accessing data in a user-friendly manner.[2]

8. A good analogy for the difference between the LIS database and the LIS system is that the LIS database is like a Microsoft Word document file (a .docx file) and the LIS system is like the Microsoft Word software system. All the content of the document exists in the .docx file, but for ordinary users to easily view, modify, or print that file, they would need a working Microsoft Word system. Similarly, for ordinary users to use the LIS database, they would need a working LIS system. A technical user or a computer-forensics specialist with the appropriate skill set, however, could view and extract data from the LIS database without the LIS system just as such a technical user could view a Microsoft Word document without a working Microsoft Word system. For a technical user, the LIS database would be easier to get up and running compared to the LIS system, because the LIS database had fewer dependencies on software, no dependencies on hardware, and few if any dependencies on the Theranos' IT infrastructure. The usability and recovery difficulty for the LIS database compared to the LIS system is summarized in the following table:

[1] Ex. C (10/29/20 Letter from the Government) at 21.

[2] Ex. D (Theranos' Response to PFM's Interrogatory No. 54) at 5–8.

	Usability	Recovery Difficulty
LIS Database	By Technical User	Easy
LIS System	By Ordinary User	Medium

Table 1: Comparison of LIS Database and System

V. CLEARING UP THE CONFUSION OVER ENCRYPTION AND THE LIS DATABASE

9. In my review of the materials listed in Exhibit B, I have found that there was considerable confusion on the part of the government and the witnesses it interviewed about encryption and the LIS database. For instance, Eric Caddenhead, a former Theranos IT employee who worked there as an IT Architect told a Theranos' IT consultant in August 2018 that "if they took the LIS apart they would not be able to access it again because then the encryption key would be lost. The encryption key was located on a disk array which had a lot of pieces and when they took the disk array apart it would have destroyed the encryption key."[3]

10. The Court appeared to accept this view put forward by the government in its Order denying Ms. Holmes motion to suppress anecdotal data.[4] The Court observed—based on the government's submissions—that Theranos' counsel, WilmerHale, "failed to mention [to the government] that a private key would also be necessary to access the LIS database."[5] The Court ultimately determined that it was undisputed between the government and Ms. Holmes that "the only entity in possession of the sole working version of the LIS database was Theranos—up until it dismantled the database hardware, destroying the key and *rendering the original database unusable as well*."[6]

11. The government's conclusion and assertion that it would have needed an encryption key after Theranos disassembled the LIS system at the end of August 2018 is

[3] Ex. E (US-REPORTS-0016251) at 3.
[4] Order at 6, Dkt. No. 887.
[5] Order at 5, Dkt. No. 887.
[6] Order at 12, Dkt. No. 887 (emphasis added).

incorrect, and reflects fundamental misunderstandings of the system and encryption. Within the LIS system—composed of servers and disk storage, the database, and software to access it—there are several instances of encryption being used to protect the data: (1) certificate-based encryption of the database called Transparent Data Encryption (TDE);[7] (2) document encryption via Active Directory Rights Management Services (AD RMS); (3) document encryption protected by document passwords;[8] and (4) password encryption of private encryption keys.[9] My review of the evidence shows that the government and witnesses it interviewed confuse these encryptions. The government's theory, accepted by the Court in connection with Ms. Holmes' motion to suppress, was that a missing password for the private encryption key (number 4 in the preceding sentence) prevented access to the data. But this password for the private encryption key would have been necessary only for accessing data from the LIS database backup that Theranos produced to the government in August 2018. The missing password for the private encryption key ***would not*** have been necessary had the government obtained possession of the equipment running the LIS database either before or after August 31, 2018. Unlike with the LIS database backup produced by Theranos, possessing this equipment would have allowed access without any password for the private encryption key. I understand that the government had the ability to seize evidence in the event that Theranos declined to cooperate in transferring possession to the government.

12. Recovering either the LIS database or the LIS system did not turn on possessing the missing password for the private encryption key. Instead, the government appears to have misunderstood two important facts. First, that the LIS database and LIS system remained on the LIS equipment both before and after that equipment was disassembled in August 2018. And second, that by obtaining the equipment, the government could have recovered either or both the LIS database and the LIS system.

[7] Ex. F (TheranosABC00037962).

[8] Ex. G (US-REPORTS-0019711) at 3 ("This document was an Excel document, which was encrypted through Microsoft RMS. CADDENHEAD ended up getting a copy of the Excel document, but could not get into it because he did not have the password to the document.").

[9] Ex. F (TheranosABC00037962) (See "ENCRYPTION BY Password").

13. Either before or long after August 31, 2018—when Theranos shut down and disassembled the LIS system[10]—the government could have obtained possession of the LIS production equipment—i.e., the servers, storage and related hardware that ran the LIS system. Before August 31, 2018, all parties agreed that the LIS system was up and running with at least one user.[11] The level of effort and technical skill would have been much the same if the government had acted to take possession of these items either before or during the lengthy period after August 31, 2018. Because the data remained on the LIS system equipment, the government could have recovered the LIS database either by accessing that equipment at Theranos before it was disassembled or by obtaining the same equipment after disassembly.

VI. THERANOS DID NOT DESTROY THE LIS EVIDENCE

14. Contrary to the government's claims,[12] Theranos did not destroy the LIS database or the LIS system when it disassembled the LIS system equipment at the end of August 2018. Instead, the available evidence shows that Theranos preserved and protected it.[13]

15. After disassembling the LIS system equipment, the disk drives containing the LIS database and system were preserved and stored offsite after August 31, 2018, it appears at an Iron Mountain storage facility.[14] It also appears that the equipment (servers and other hardware) and the hard drives that contained the LIS database were also placed in storage.[15] I am aware of

[10] Ex. G (US-REPORTS-0019711) at 4 ("On Friday August 31, 2018 the Newark facility was shut down. . . .").

[11] Ex. H (US-REPORTS-0016262) at 4 ("CHUNG recalled that right before they shut down the LIS to move it, someone from Theranos told them to wait because they had to pull one more report from LIS. Someone had made an announcement that the LIS was being shutdown and they wanted to wait until everyone was ready to shut it down.").

[12] Dkt. 846 at 2, lines 6–7; Dkt. 682 at 7, lines 13–16 (claiming that "by August 31, 2018, the database had been completely shut down" and that afterward, "the data was gone").

[13] Ex. I (TheranosABC00039050).

[14] Ex. J (WH000000970) (second in email thread, "Theranos has preserved its various databases, including the LIS database, on hard drives and plans to store those hard drives at Iron Mountain."); Ex. H (US-REPORTS-0016262) at 2 ("The production infrastructure stayed in storage for about a year or so, then JARED LNU (JARED) from Sherwood called because the equipment Lessor wanted their equipment back."); *id.* at 3 ("CHUNG's team went to storage and confirmed the equipment was there, but found that all the hard drives had been removed.").

[15] Ex. H (US-REPORTS-0016262) at 3 ("CHUNG then recalled MCCHESNEY had asked him and his team to remove all the hard drives before they were placed on the truck. The hard drives were packed in separate boxes and taken to a different storage facility, but CHUNG did not know where they were taken.").

nothing that would have stopped the government from obtaining possession of either or both the disk drives and server equipment before or long after August 31, 2018.

VII. CONFIGURATION OF THE EQUIPMENT RUNNING LIS

16. The equipment running LIS at Theranos appears to have been in the form of a single computer rack, similar to Figure 1 below.[16]

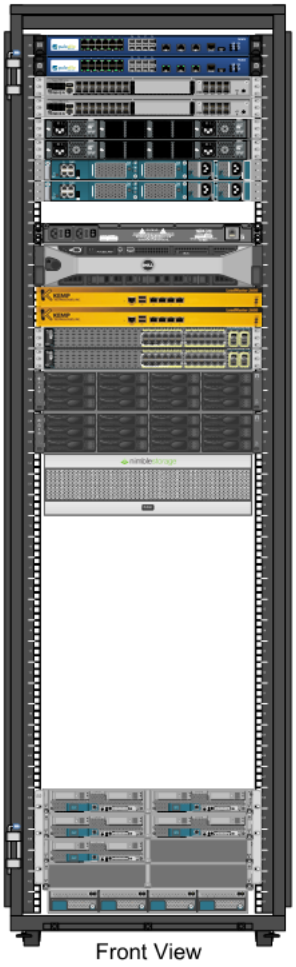


Figure 1: LIS System Equipment Rack

[16] Ex. K (BALWANI000001–BALWANI000003) (Email and attached Visio file); *see also* Ex. L (THPFM0000650372) at 3. The inventory I reviewed included the vendor service tags providing a complete itemized list of the hardware as it was originally shipped to Theranos. *See id.*

VIII. RECOVERING THE LIS DATABASE BY OBTAINING PRODUCTION EQUIPMENT BEFORE OR AFTER AUGUST 31, 2018

17. The LIS database was active and operating before August 31, 2018. There would therefore not have been any issues with accessing the data stored in it had the government either accessed the data onsite at Theranos or obtained the equipment for transport to a government facility. I have seen nothing to suggest that Theranos or its law firm WilmerHale would not have cooperated by providing any user IDs and passwords or creating any new users needed, but I understand the government could have used coercive methods as well. The government has never claimed that the IT professionals it interviewed lacked administrative passwords to the system or would not have supplied those upon request. These passwords are completely different from the missing private encryption key. Even without obtaining the administrative passwords through cooperation or coercion, with physical possession of the equipment, a technical specialist could have accessed the LIS database with forensic tools and obtained the required user IDs and passwords. No private encryption keys would have been needed because such keys were in place on the seized equipment. For that reason, the LIS data could have been reviewed and extracted by a technical user with skills like my own.

18. In denying Ms. Holmes' motion to suppress (Order, Dkt. No. 887), the Court concluded—based on the government's representations—that the government's conduct *after* August 31, 2018, is "irrelevant."[17] This conclusion turned on accepting that the government could not have reconstructed the LIS database because Theranos' dismantling of the LIS system equipment permanently eliminated the ability to access data without the private encryption key.[18] The government's claims in this regard are incorrect.

19. After August 31, 2018, the LIS system had merely been disassembled with the hard drives stored in one location and the rest of the equipment stored in another.[19] A technical specialist could have readily reassembled the LIS system from these stored components; and then

[17] Order at 14, Dkt. 887.

[18] Order at 13, Dkt. 887.

[19] Ex. H (US-REPORTS-0016262) at 3–4.

this scenario would have been the same as recovering the LIS database before August 31, 2018. Michael Chung, a consultant with a company called Neetek that was working with Theranos in 2018,[20] was incorrect when he stated that "once the hard drives were taken out of the servers, if they were not tracked as to where they came from, it would have been impossible to put them back together. Even if the hard drives were all labeled correctly, it would have been extremely difficult to reconstruct the database because in addition to the servers there are also hundreds of network devices which would have to be connected correctly."[21] While labeling all the disk drives before removal might have reduced the recovery time, it was not essential since each disk drive could have been examined forensically to determine its placement. Most of the disk drives were for the Dell EqualLogic storage array. EqualLogic stores metadata on the disk drives themselves so when returned to the array, the array controller reads the metadata from each disk drive and restores them to their configuration when they were removed. The other disk drives are mirrored boot drives for the servers and those can be examined and recovered as well. Mr. Chung's stated concern over "network devices" would not have applied to the recovery of the LIS database.

IX. RECOVERING THE LIS SYSTEM BY OBTAINING PRODUCTION EQUIPMENT BEFORE OR AFTER AUGUST 31, 2018

20. The government could have also recovered the LIS system and not just the database if it had acted to do so before or after August 31, 2018. When interviewed by the government, Mr. Chung thought that "[i]t would have been a gargantuan effort to rebuild this system from scratch. However, they would need the encryption key."[22] Mr. Chung's statement is incorrect in regards to the production equipment. With the original hard disk drives, which were placed in storage after August 31, 2018, [23] the LIS system could have readily been reassembled to

[20] *Id.* at 1 ("The first work CHUNG did for Theranos was to move servers. In July 2018 CHUNG met with JOHN MCCHESNEY (MCCHESNEY), who had contacted Neetek, in regards to moving servers from Newark to a datacenter as Theranos was trying to get out of their Newark facility.").

[21] Ex. M (US-REPORTS-0025153) at 5.

[22] Ex. N (US-REPORTS-0019324) at 6.

[23] Ex. J (WH000000970) (second in email thread, "Theranos has preserved its various databases, including the LIS database, on hard drives and plans to store those hard drives at Iron Mountain.").

allow access to and retrieval of the laboratory data with user-friendly functionality. While all the LIS system hardware (disk drives, servers, and so on) were in Theranos' storage facilities,[24] it would have been a straightforward technical task to reassemble the LIS system, and no password for the private encryption key would have been needed. As noted above, reassembling the LIS system for use by an ordinary user would have been a more time-consuming task compared to setting up LIS database access for a technical user.

X. CONCLUSIONS

21. I conclude that no private encryption key would have been needed had the government pursued either accessing the LIS database or the LIS system by obtaining possession of the hard disk drives and equipment that ran the LIS instead of just the LIS database backup provided to it by Theranos. The government could have accessed and obtained the LIS data by obtaining the LIS equipment either before or long after August 31, 2018. Claims by the government to the contrary in the material I reviewed are incorrect.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 19th day of November, 2021 at Houston Texas.

Richard L Sonnier III
RICHARD L. SONNIER III

[24] Ex. O (US-REPORTS-0025177) at 4; Ex. P (DTTPROD-00000159).

EXHIBIT A

Richard L Sonnier III - Curriculum Vitae

nimbleservices.com/about/richardcv

Nimble Services Inc.
1519 Roy Street,
Houston, TX 77007
Phone: 281-445-4800
Email: rsonnier@nimbleservices.com

Summary of Qualifications

I bring over 29 years of experience and skill to Nimble Services' customers who need cost effective computer systems and networks. I create solutions across a multitude of computer platforms and network technologies and focus on solutions with longevity based on industry standard technology.

Analyze and Design

- High performance computer infrastructures integrated with legacy systems
- High speed LANs/WANs/SANs and client/server architectures using Ethernet (10/100/1000) Switches, Routers, TCP/IP, Frame Relay, T1/T3, FDDI, Fibre Channel, TCP/IP, and the Internet

Secure

Computer security including audit preparation, audit remediation, penetration testing, policies and procedures

Integrate

- UNIX, NT, Solaris, HP-UX, AIX, IRIX, SCO, Digital UNIX, UNICOS, MPE/iX, MVS, Linux, and Windows networks into coherent company information system
- Standard and custom solutions with BMC ASA software: Patrol, BEST/1, SQL*Backtrack

Implement

- Computer systems management including policies, procedures, knowledge transfer, and products

- Network services: distributed backup, network printing, E-mail, security, universal file and data access, ORACLE, SQL Server, AFS, NFS, DFS, Samba, www, ftp, and high availability servers

Troubleshoot

All aspects of complex networked systems focusing on increased performance and seamless ease of use

Develop

Custom system services and applications to provide complete computing environment in C, C++, FORTRAN, Visual BASIC, Pascal, LISP, Korn, Perl, TCL/TK, SQL, NT Batch, Java, JavaScript, and PowerShell

Manage

Complex systems integration and management projects

Biography

I am the co-owner of the Nimble Services, Inc. based in Houston, Texas. I graduated from Louisiana State University in 1985 with a B.S. in Physics and second B.S. in Computer Science, and I have over 29 years experience designing technical computing solutions.

I began my professional career at Litton Industries supporting a US Navy contract creating a large database of warship design and support data. I was responsible for all aspect of the system: database, data storage, high-speed networking, imaging and scanning, and data visualization. I developed and implemented operational support systems and data converters. In my last assignment with Litton, I was the DB2 Database Administrator for a large business unit.

After leaving Litton, I moved to Houston, TX and took a contract position with Exxon Corporation. Over the next ten years, I worked on numerous data storage and migration projects including a custom HSM system that migrated data from Apollo and Sun workstations to a large IBM mainframe attached to a very large tape storage facility and a large AFS implementation that scaled from a few hundred Gigabytes to 4 Terabytes during my tenure. I designed, developed and implemented the backup system for Exxon's AFS site using up to 8 DLT tape jukeboxes. Additionally, I served on the evaluation team that extensively tested all the major enterprise RAID storage products of that time. Ultimately, Data General Clarrion systems were selected and I was instrumental in rolling out the new system to a capacity of 25 Terabytes. Also, I connected the Netscape web server to Exxon's AFS data via a custom security plug-in and implement one of the first web search engines deployed in Exxon.

While contracting at Exxon, I joined a start-up company, Paranet, as its first employee. At Paranet I was a technology leader and advised many project teams. I managed the development of two commercial software products. One was a geophysical map data converter that was very successful. The other was a data backup system that was one of the first systems to support the new 8mm and 4mm tape stackers and jukeboxes. This backup system was sold to Exxon and used in production for several years. Additionally, I developed a custom driver for EPOCH Systems' InfiniteStorage Architecture to allow data backup and archive of Apollo workstation data to EPOCH systems.

After leaving Paranet, I co-founded Net Partners, Inc. where I continued to work on data converters for geophysical data and worked on many other types of information technology projects. My last project at Net Partners was leading a team to develop a seismic data processing collaboration platform for a seismic processing vendor. The project allowed seismic data to be processed and interpreted remotely over the Internet with a web browser. I designed and implemented the entire data management subsystem including the relational database. Also, while at Net Partners, I specialized in computer system performance analysis and capacity planning. I completed many performance-troubleshooting projects often involving large ORACLE databases, and I trained BMC Software's class instructors on BEST/1, BMC's well-known performance and capacity planning tool.

After leaving Net Partners, I founded Nimble Services, Inc. where I continued to develop and lead cutting edge information technology projects including:

- Converting a Microsoft Access application into a web-based solution serving a community of global users for a major chemical company.
- Developing many web-based interfaces to legacy computer applications and databases running on mainframe or minicomputers.
- Scaling up web application infrastructure to support thousands of users using clusters of application and database servers with secure, redundant firewall front-end systems.
- Designing high performance computer networks.
- Migrating legacy IT applications and systems to modern web-based solutions.

Experience

IT Security:

- Access Control Systems and Methodology
- Designed and implemented numerous security schemes to meet client needs using user IDs, security groups and ACLs available in most operating systems.
- Audited access control systems and security at many sites.
- Implemented custom password complexity programs at several clients.
- Analyzed password strength using cryptographic analysis and brute force attacks.

- Engineered solutions to eliminate clear text passwords in applications and databases using security standards and custom programs to encrypt passwords.
- Extended applications like web servers to use advanced system security features like Kerberos Authentication and ACLs.
- Unified access control across the network by integrating Windows, UNIX and other computer security.

IT Security:

- Telecommunications and Network Security
- Performed security penetration test including Internet, WAN and LAN.
- Developed custom firewall solutions based on the Linux operation system.
- Secured Internet access with firewalls: FWTK, MS Proxy Server, Cisco PIX/ASA, CheckPoint, NetScreen, NetMax, SonicWall, Linksys, routers and other network security devices.
- Evaluated firewall effectiveness and reported on the results.
- Performed TCP/IP network performance tests.
- Analyzed security incidents at many companies including ExxonMobil, Global Marine and Universal Weather.

Business Continuity Planning and Disaster Recovery Planning

- Developed business continuity plan for UNIX systems at several clients
- Implemented failover solutions including clusters and data replication.
- Designed hot and cold backup sites for several clients including network, hardware, software and security aspects.

Security Management Practices

- Presented security best practices to CIO level executives and IT staff at several clients.
- Trained IT staff on security management and maintenance.
- Presented on computer security at conferences like Houston Business Expo and GHRUG.

Security Architecture and Models

- Created security audit scripts to maintain compliance.
- Implemented audit remediation to comply with corporate policies.
- Developed SOX audit policies and procedures.
- Developed tax compliance system to track corporate tax filings and compliance.
- Conducted numerous Technical Control Analysis Processes (TCAPs) on many IT products and services for ExxonMobil. TCAP is ExxonMobil's security evaluation and audit process to ensure all IT products and services comply with corporate standards and policies.

- Designed ExxonMobil's B2 level security environment for its exploration company covering systems, software, networks and security training.
- Audited security practices against business policies at several clients including ExxonMobil, Global Marine, and Challenger Mineral.

Legal Analysis

- Performed forensic analysis of many systems and provided expert reports for 8 or more legal cases dealing with theft of intellectual property, serving as expert witness in several cases.
- Provided expert analysis and reports for a software patent case. This expert witness analysis was cited by the Circuit Court of Appeals in a successful appeal of the case and instrumental in the favourable outcome for the client: http://www.cafc.uscourts.gov/opinions/06-1440.pdf

Application and Systems Development

- Developed application level network security solutions where remote systems were granted access to mainframe resources based on their physical IP address and two factor user authentication.
- Developed web-based application requiring SSL security.
- Converted a low security commercial web server farm to higher security farm located in a physically secure co-location facility and designed remediation solutions to fix 90% of the risk exposures.
- Developed a security framework to improve security of the web-based applications.
- Integrated, programmed and managed IBM Series/1 computers that linked the IBM mainframe with machine tools on the manufacturing floor.
- Integrated several manufacturing floor systems with HP 3000 mainframe and later HP-UX server including shop scheduling system, labor data collection system, and DNC machine tools.
- Designed and developed the operating system based on Linux for custom manufacturing floor terminals.
- Developed custom data communication protocols for communication between the HP 3000 mainframe and the manufacturing servers running over both Ethernet and RS-232 serial links with full redundancy, failover and failback.
- Developed support software for testing of Blue Sky's custom TDC for high end physics experiments (STAR TOF experiment of the Relativistic Heavy Ion Collider at Brookhaven National Laboratory) in LabWindows/CVI.
- Managed the development team for Blue Sky's follow-up software to support their TDC including recruiting the team, designing the software, and debugging it.
- Developed the device driver for Blue Sky's line of high performance waveform digitizers as well as some parts of the firmware and VHDL for the PCI-E interface.

- Analyzed patents on embedded systems in vehicles and how those systems form a distributed multiprocessor system via an open communication system.
- Analyzed the source code for numerous electronic control units (ECU's) found in Ford vehicles especially how they communicate over the CANbus to form a loosely connected distributed multiprocessor system.
- Analyzed the specification and schematics of the electronic components installed in Ford vehicles known commercially as Ford SYNC; and how those components are linked to other systems including Ford SYNC services.
- Inspected and tested various combination of Ford ECU's on vehicle bucks.

IT Infrastructure

- Managed technical tools for support personnel.
- Enhanced sales with technical support and technical information.
- Improved customer service levels by increasing site efficiency.
- Developed Help Desk and Network Inventory service offerings.
- Developed an AFS backup system.
- Configured Internet mail gateway and MS Exchange to support SMTP mail for 400 Exchange users.
- Managed the corporate network of Suns, HPs, Macs and PCs.
- Implemented a command line interface to TCP/IP sockets for UNIX systems.
- Implemented a UNIX and PC integration project using PC/TCP.
- Developed a UNIX file archival system using TCP/IP.
- Designed LAN and WAN networks with 100's of nodes using TCP/IP, IPX, and SNA protocols.
- Configured NFS for Suns tied to Apollo networks.
- Administered an IBM DB2 relational database system on a 4381.
- Created relational databases in ORACLE on a VAX VMS system.
- Administered a 50 node Apollo network with over 100 users.
- Administered a Empress relational database system.
- Tested new CAD software.
- Supported Versatec and HP plotters.
- Supported Optigraphics system and scanner.
- Supported the Symix/Syteline ERP, engineering design systems, and the manufacturing floor electronic test equipment and the integration between them.

Business Systems Development

- Implemented Compiere ERP on ORACLE 9 and 10.
- Developed an engineering drawing control system.
- Developed a multi-media web application providing audio, video and application windows to remote Internet users.
- Setup UltraSeek Internet search engine to index and search corporate information.

- Administrated SQL Server and Net Dynamics server for database oriented Web applications.
- Improved a backup product with 8mm tape support on DOMAIN/OS and AFS support for Suns.
- Managed a geophysical map converter development team and developed the core application framework for the product.
- Developed a user interface for a GeoShare converter product.
- Developed a converter for 3D manufacturing data between Computer Vision and Calma CAD/CAM systems.
- Managed a CAD installation project that installed 3 division networks.
- Designed and implemented GUIs in DOMAIN/Dialog, Open Dialogue, X11, and OSF/Motif.
- Implemented TCP/IP to SNA gateways.
- Developed an IOS type manager for backing up Apollo networks to an IBM mainframe.
- Developed a color raster formatter for a Versatec 3444 plotter.
- Developed a user support/problem tracking system.
- Introduced software engineering techniques into CAD project.
- Developed a custom IBM/RJE server.
- Developed a plot control/management system.
- Developed a generic mailbox communications package.

Performance and Monitoring

- Developed a network monitoring application that used audio recording and playback for messaging.
- Fixed ORACLE SQL*Net operations and performance.
- Analyzed X11 performance over Frame Relay network.
- Developed a UNIX system performance tool.
- Created and taught computer performance classes features BMC’s BEST/1 product.
- Analyzed the performance of databases, networks, clients and applications providing recommendations to increase performance and resolve bottlenecks.

Conversions

- Converted UNIX web server to NT 4.0 and IIS.
- Ported an application from DOMAIN/OS to HP-UX.
- Converted data from numerous different systems to new formats.
- Developed an HP 3000 MPE emulation layer to port an entire suite of business application from MPE to HP-UX.

Expert Witness Cases

Testifying

- AllVoice Computing PLC v. Nuance Communications, Inc.
- AirGas, Aeriform v. IWS Gas and Supply
- JOHN C. MITCHELL, ALAN J. HEARD, STEVEN N. CORBETT, and NICHOLAS J. DANIEL v. DOUGLAS HOLT, MICHAEL K. DAVIS, and JOSEPH H. MIGLIETTA
- ALLVOICE DEVELOPMENTS US, LLC v. MICROSOFT CORPORATION

Consulting

- EAGLE HARBOR HOLDINGS, LLC, and MEDIUSTECH, LLC v. FORD MOTOR COMPANY
- WCS v. TMI
- OmmiLabs v. Core Lab
- POLYDYNE SOFTWARE INC. v. CELESTICA INTERNATIONAL, INC.

Forensics

- James Roll vs GCA Services Group
- Jacintoport vs former employees
- AET vs C5 Communications, Eric Smith, et al.
- US Quality Furniture of Services Inc. vs Furniture Works Inc.
- Sanitors Services Inc. vs Nathaniel B. Shaw
- BASEOPS INTERNATIONAL, INC. VS. EDUARDO HERNANDEZ, INTERNATIONAL TRIP PLANNING SERVICES LLC, INTERNATIONAL TRIP PLANNING, LLC and MGAS GLOBAL AVIATION SERVICES LLC
- Brad Randell
- Conix
- GAO
- Massage Envy Imperial Oaks
- Boulevard Reality/Sudhoff
- Beacon Medical v. Steve Sullivan
- PointServe (Mobi) v. IPX
- Trading Technologies International, Inc. Patent cases
- T & T Engineering Services, Inc. v. Axel Michael Sigmar, et al

Employment

- Nimble Services Inc., Founder, President & Senior Systems Analyst 2001-Present
- Net Partners, Inc., Co-founder, Senior Partner 1993-2001
- Paranet, Inc., Senior Systems Consultant 1991-1993
- Prime Computer, Inc., Systems Integration Consultant 1990-1991
- Exxon Company, USA Systems Analyst (contract) 1988-1990
- Litton Industries, Inc., Systems Programmer/Analyst 1986-1988

Education

- Louisiana State University, B.S. Computer Science 1985
- Louisiana State University, B.S. Physics 1985
- University of Southern Mississippi, Graduate courses: Relational Database Systems and Software Engineering 1987
- Tulane University A. B. Freeman School of Business, Master Certificate in Business Management 2005

Continuing Education

- BMC Patrol Administration/Implementation
- Microsoft Windows NT Programming
- Developing File Systems for Windows NT
- BEST/1 for UNIX
- BEST/1 for Distributed Systems SureStart Engagement Process
- FileNET Panagon Sys Admin on UNIX
- OSF DME Workshop
- OSF DCE Internals
- Tivoli Management Environment Advanced Developer
- Advanced Perl Programming
- Mach 3.0 MIG Programming
- Porting the Mach 3.0 OS
- OSF/1 Introduction
- Project Management
- Parallel Algorithms and Architectures for 3D Image Generation
- X-Windows and Open Dialogue Programming
- Network Computing System (NCS) Programming
- MVS/XA Introduction
- IBM Series/I CF Support
- IBM Series/I EDL Programming
- Calma Apollo DDM System Support
- Introduction to Hypertext and Hypermedia

Publications

- UNIX Review, “Spotlight on FDDI” October, 1992
- LISA IV, “TCL and Tk: Tools for the System Administrator” October, 1992

Houston Business Review, Cost Effective IT series of articles, 2004-2005

- Cost Effective IT
- Cost-Effective IT 100 Megabit Wireless
- Cost-Effective IT Are PCs Getting Easier To Use

- Cost-Effective IT Auditing
- Cost-Effective IT Cell Phone 2005
- Cost-Effective IT Cell Phone Applications
- Cost-Effective IT Compiere
- Cost-Effective IT Cost Savings
- Cost-Effective IT EBusiness
- Cost-Effective IT Easy To Use Software
- Cost-Effective IT For Marketing Your Business
- Cost-Effective IT Future Technology
- Cost-Effective IT Hardware Failures
- Cost-Effective IT Hardware Trends
- Cost-Effective IT High Speed Wireless
- Cost-Effective IT In Emergencies
- Cost-Effective IT Internet Future
- Cost-Effective IT Internet Security
- Cost-Effective IT Linux And Open Source 2005
- Cost-Effective IT Mozilla Thunderbird
- Cost-Effective IT Netscape Reborn
- Cost-Effective IT Network Storage
- Cost-Effective IT New Developments March 2004
- Cost-Effective IT New Sales Software
- Cost-Effective IT Nvu
- Cost-Effective IT Offshoring
- Cost-Effective IT Open Source Compiere
- Cost-Effective IT Photo No No
- Cost-Effective IT Planning
- Cost-Effective IT Planning For New Year
- Cost-Effective IT Policies Procedures
- Cost-Effective IT Security Part One
- Cost-Effective IT Security Part Three
- Cost-Effective IT Security Part Two
- Cost-Effective IT Service Oriented
- Cost-Effective IT Software Failures
- Cost-Effective IT Stopping SPAM
- Cost-Effective IT Successful Ventures
- Cost-Effective IT The Business Process
- Cost-Effective IT The Compiere Difference
- Cost-Effective IT The Compiere Difference NEXT
- Cost-Effective IT The Dark Side
- Cost-Effective IT Tough Decisions
- Cost-Effective IT User Failures
- Cost-Effective IT Web Applications

- Cost-Effective IT Web Based Training
- Cost-Effective IT Web Development and Dreamweaver
- Cost-Effective IT Web Forms
- Cost-Effective IT Wireless Networking
- Cost-Effective IT Wireless Inventory

Other Skills

Houston Business Show on CNN 650 Radio, Periodic Appearances and Guest Host, 2004-2005

References

Available upon request.

EXHIBIT B

EXHIBIT B

Beginning Bates	Date	Description
PLEADINGS		
n/a	11/20/2020	Holmes's Motion to Exclude Evidence of Anecdotal Test Results
n/a	1/11/2021	USA's Corrected Opposition to Motion to Exclude Evidence of Anecdotal Test Results
n/a	2/23/2021	Holmes's Reply ISO of Motion to Exclude Evidence of Anecdotal Test Results
n/a	6/2/2021	Motion to Suppress Evidence of Customer Complaints and Testing Results as Well as Finding in CMS Report
n/a	6/2/2021	Wade Declaration ISO of Motion to Suppress
n/a	6/21/2021	Opposition to Motion to Suppress
n/a	6/21/2021	Bostic Declaration ISO Opposition to Motion to Suppress
n/a	6/28/2021	Reply ISO Motion to Suppress
n/a	6/28/2021	Wade Declaration ISO of Reply ISO Motion to Suppress
n/a	8/4/2021	Order Denying Motion to Suppress
TheranosABC00042260	8/8/2018	Leach Decl., Ex. 70, Dkt. No. 681-34 (Email from Xan White to WilmerHale re: Re: LIS data base discussion - response to request) (GTX 4762)
n/a	9/28/2020	Leach Decl. Ex. 72, Dkt. No. 681-36 (Sept. 28, 2020 expert witness report of Bruce W. Pixley)
n/a	7/23/2020	Saharia Decl., Ex. 101, Dkt. No. 735-2 (Letter from R. Leach to K. Trefz responding to July 7, 2020 letter regarding Rule 16 productions)
DEPOSITION TRANSCRIPTS		
n/a	4/24/2019	Deposition transcript of Shekar Chandrasekaran, In re Arizona Theranos, Inc. Litigation
n/a	4/23/2019	Deposition transcript of Sekhar Variam, In re Arizona Theranos, Inc. Litigation
DISCOVERY		
n/a	12/12/2016	Theranos's Response to PFM's Interrogatory No. 54
LIS APPLICATION USER GUIDES		
THPFM0001705425	6/9/2015	Theranos LIS Application June 9th, 2015 Release presentation
THPFM0003358957	10/20/2015	LIS App User Guide presentation
THPFM0003358959	10/20/2015	Customer Service App User Guide presentation
THPFM0000091880	11/15/2015	Standard Operating Procedure Theranos SW Qualification and Qualification Report Accessioning Application, Bridges Application, and LIS Application Qualification
CORRESPONDENCE		
n/a	10/29/2020	Letter from Robert Leach to Lance Wade re: Brady information
MEMORANDA OF INTERVIEWS		
FBI-AUDIO-000001	12/9/2020	Shekar Chandrasekaran FBI interview audio file
US-REPORTS-0024254	12/9/2020	Shekar Chandrasekaran Memorandum of Interview
US-REPORTS-0016258	4/23/2020	Antti Korhonen Memorandum of Interview
FBI-AUDIO-000002	7/27/2020	Antti Korhonen FBI interview audio file
US-REPORTS-0017921	7/27/2020	Antti Korhonen Memorandum of Interview
US-REPORTS-0016262	4/23/2020	Michael Chung Memorandum of Interview
FBI-AUDIO-000003	10/6/2020	Michael Chung FBI interview audio file
US-REPORTS-0019324	10/6/2020	Michael Chung Memorandum of Interview
PROFFER-000032	11/25/2020	Michael Chung Attorney Proffer
US-REPORTS-0025153	12/7/2020	Michael Chung Memorandum of Interview
US-REPORTS-0016251	4/16/2020	Eric Caddenhead Memorandum of Interview
FBI-AUDIO-000004	10/7/2020	Eric Caddenhead FBI interview audio file
US-REPORTS-0019711	10/7/2020	Eric Caddenhead Memorandum of Interview
US-REPORTS-0019703	10/14/2020	Eric Caddenhead Memorandum of Interview
US-REPORTS-0019683	10/15/2020	Eric Caddenhead Memorandum of Interview

EXHIBIT B

Beginning Bates	Date	Description
US-REPORTS-0020386	11/2/2020	John McChesney Memorandum of Interview
US-REPORTS-0020367	11/12/2020	Mike Wei Memorandum of Interview
US-REPORTS-0020410	10/16/2020	Alexander (Xan) White Memorandum of Interview
US-REPORTS-0019170	10/27/2020	Alexander (Xan) White Attorney Proffer
US-REPORTS-0019706	11/2/2020	Alexander (Xan) White Attorney Proffer
US-REPORTS-0019708	11/2/2020	Alexander (Xan) White Attorney Proffer email
US-REPORTS-0025177	12/17/2020	Jarod Wada Memorandum of Interview
US-REPORTS-0020373	10/14/2020	Wilmer Hale Attorney Proffer
US-REPORTS-0025513	2/18/2021	David Taylor Attorney Proffer
EMAIL		
WH000002070	5/23/2018	Email from Mike Romeo to David Taylor, Christopher Davies, Michael Mugmon, Matthew Benedetto and Katie Moran re: Theranos - Summary of 5/23/18 Call with the DOJ
TheranosABC00039050	6/22/2018	Email string between Eric Caddenhead and Xan White re: Summary of our conversation [privileged/confidential]
TheranosABC00039916	7/30/2018	Email string between John McChesney, Eric Caddenhead, Xan White, and David Taylor re: LIS data base discussion - response to request
CHUNG-EMAILS-000246	8/6/2018	Email string between John McChesney, Michael Chung, and Xan White re: LIS Copies - need Eric or Antti
WH000002324	8/8/2018	Email string between Xan White and Katie Moran re: LIS data base discussion - response to request
TheranosABC00037454	8/11/2018	Email string between Craig Josephson, Xan White, Michael Chung, John McChesney, Eric Caddenhead and David Taylor re: Theranos - LIS Database Copy Update 2
WH000003587	8/24/2018	Email from David Taylor to George Schuster, Benjamin Loveland, Isley, Gostin, Michael Mugmon, Katie Moran, Mike Romeo, and Xan White re: Email
CHUNG-EMAILS-000574	8/30/2018	Email string between Eric Caddenhead, Michael Chung, Shekar Chandrasekaran, John McChesney and David Taylor re: LIS
TheranosABC00038585	8/30/2018	Email string between Sekhar Variam, David Taylor, Eric Caddenhead and Shekar Chandrasekaran re: LIS data base discussion - response to request
TheranosABC00037345	9/2/2018	Email string between David Taylor, Michael Chung, Eric Caddenhead, Shekar Chandrasekaran, and Sekhar Variam re: LIS data base discussion - response to request
TheranosABC00037962	9/2/2018	Encrypt_SQL_Databases_Staging.docx (decrypted)
TheranosABC00038253	9/2/2018	Email string between Shekar Chandrasekaran, David Taylor, Michael Chung and Eric Caddenhead re: Info for Shekar
WH000000970	9/14/2018	Email string between Roger Heller and Stephen O'Neill re: In re Theranos: Request for Confirmation re Preservation of Evidence
DTTPROD-00000159	10/12/2018	Email between Jarod Wada, Michael Chung, David Taylor and Phillipe Poux re: Theranos ABC - Cisco capital lease equipment
TheranosABC00001770	11/7/2018	Email string between Mike Wei and Jarod Wada re: Theranos LIS database
WH000000669	7/30/2019	Email from Mike Romeo to John Bostic and Jeffrey Schenk re: Theranos GJ subpoena response
NETWORK SCHEMATICS AND INFORMATION		
THPFM0000228604		Network diagram
BALWANI000001 - BALWANI000003	6/10/2015	Email from Ian McDowell attaching Visio's of the rack config and connectivity map (native files)
THPFM0000650372	3/12/2013	Dell Master Lease Agreement
LIS Hard Drive		
HARD-DRIVE-LIS-000001		AllKeys_Certs.zip

EXHIBIT B

Beginning Bates	Date	Description
PUBLICLY AVAILABLE DOCUMENTS		
	Public information from Dell related to the Dell Master Lease Agreement (THPFM0000650372), available at https://nimbleservice-my.sharepoint.com/:f:/g/personal/rsonnier_nimbleservice_onmicrosoft_com/EiYoyWqZSu1KtUqPxLT-gcMBSy0XNSy2Va8GgaJbQJtUfg	
		1CSNZX1.xlsx
		9BSNZX1.xlsx
		BBSNZX1.xlsx
		CBSNZX1.xlsx
		DBSNZX1.xlsx
		FBSNZX1.xlsx
		GBSNZX1.xlsx
		GN8MDV1.xlsx
		JBSNZX1.xlsx
	Public information from Dell, other vendors, and other websites, available at https://nimbleservice-my.sharepoint.com/:f:/g/personal/rsonnier_nimbleservice_onmicrosoft_com/EgzKYS8u3FlNqD6aYHDUK9EBGb491boa4suKXH5hk4G-Sw?e=6sKOBm	
		BestPracticesforSeizingElectronicEvidence.pdf
		Dell M Series Blade IO Guide July 2016.pdf
		Dell_PS6210_Series_Spec_Sheet_102913.pdf
		DOJ-ssmanual2009.pdf
		ESG-TechWP-Securing-EQL-SAN.pdf
		HP_Nimble_1048356599.pdf
		LawJournal-Seize First Search Later.pdf
		lightning_6gb_ds.pdf
		poweredge-m1000e_owners-manual_en-us.pdf
		recovering-windows-secrets-and-efs-certificates-offline-paper.pdf
		recovering-windows-secrets-and-efs-certificates-offline-slides.pdf
		Reference Architecture utilizing the PowerEdge M1000e Blade Enclosure SQL and Exchange.pdf
		savvio 10k5-fips-data-sheet-ds1727-4-1201.pdf
		s-solution-resources_white-papers68_en-us.pdf
		s-solution-resources_white-papers93_en-us.pdf

EXHIBIT C

United States Attorney
Northern District of California

1301 Clay Street, Suite 340S
Oakland, California 94612

(510) 637-3680
Fax: (510) 637-3724

October 29, 2020

By Email

Lance Wade, Esq.
Kevin Downey, Esq.
Amy Saharia, Esq.
Katie Trefz, Esq.
Williams & Connolly LLP
725 Twelfth Street, N.W.
Washington, DC 20005

Re: *United States v. Holmes*, CR 18-258 EJD

Dear Counsel:

Pursuant to your requests for discovery, we write to alert you to the following information, which you may view as potential *Brady*, *Giglio*, or *Jencks* information. This supplements our letter to you dated July 9, 2019. By making these disclosures, we do not necessarily agree that this information is responsive to Rule 16, *Brady*, *Giglio*, or *Jencks*, nor do we waive any applicable privilege or protection.

* * * * *

1. Government notes of a phone call with Pete Skinner on or about January 28, 2016, state in part:

> privately held
> few SHDs
>   sophisticated
>   employees
> no public offering
>
> tech
>   prop – h'ware, software, chem, protocol
> . . . .
> software enables TSPU and larger h'ware to hook up w/ cloud so machine can be used remotely & results viewed remotely
>   big data anal.

> . . . .
> co has not described to press – protocols and custom could be used by competitors
>   4 min mile
>   don't want other to reveal possibilities
> can't disclose for competitive reasons
> . . . .
> co. did not keep control systems

2. On or about May 20, 2016, an AUSA, FBI agents, and a Postal Inspector met with attorneys from WilmerHale and Boies Schiller. Notes of the meeting state in part:

> 2003-2013
>   --pharmaceutical companies
>   --small clinical lab
>   --Safeway employees blood test
> R&D lab vs. clinical lab
> now – R&D and retail operation
>   80 PhD employees
>
> Theranos tech { -collection process
>   -chemical process
>   -device
>   -software
> . . . .
> -200 tests/80 operational
> -Arizona – moderately complex
>   -not using proprietary machines
> high throughput machine – runs many at [?]

Additional notes state in part:

> 2 clinical labs: Newark, AZ
> 750 employees, 80 Phds
> 1000 patents
>
> private co.
>   85 investors
> . . . .
> barcode w patient name & test info
> create shipping container
> chemicals keep
>
> automation to industry
> . . . .
> software
>   apps for intake
>   automate lab

allows to do for less cost

cloud software – can program the TSPUs remotely
big data implication & treat in a productive way

The additional notes also reflect statements made by Theranos' counsel about efforts the company was taking in response to the CMS review and other government inquires.

3. Notes by a Postal Inspector of a call or meeting with Boies Schiller on or about June 30, 2016 state in part:

750 employees
85 shareholders
. . . .
software innovations – smaller needle & volume for venous draws
-Theranos using Edison for ELISA [?] (15 tests)
CLIA waiver for 35 machine for HSVI only

4. Notes by a Postal Inspector of a meeting with WilmerHale, the SEC, the FBI, and others state in part:

Examined – QC results,
patient distribution
proficiency testing
60,000 voided vs. 1.5 million total tests"

5. Government notes of a meeting among the government, the SEC, WilmerHale, and David Taylor dated November 16, 2016 state in part:

SB loaned $$ to the co; EH never took out
. . . .
have resources at right team

Walgreens unraveling blew all of this up

clearly errors in the lab

emphasis on Edison, TSPU, + minilab = distortion
. . . .
2007-2010: all resources into R&D
worked w/ #
established POC that the device worked
Testing more propel, more regularly would get better data
. . . .
fin record keeping not precise
. . . .
the CLIA lab misadventure

> . . . .
> 8/2014 – Wag increases projections, 500-2500
> 3 stores in PHX
> 5/14 – 20
> 41 total by 9/2014
> . . . .
> DNK why roll out stalled
> CFO issues
> new management
> failed Express Scrips

6. Notes by an SEC attorney dated December 16, 2016 of a "Call with Wilmer" state in part:

> Prosecution update
> . . . .
> Spreadsheet w/ LIS – response 14 &15 first stop
> . . . .
> LIS spreadsheet (12/9)
> 2 diff [?]

7. Notes by an SEC attorney dated December 2016 of a "Call with Wilmer Hale" state in part:

> 3. Spreadsheet – LIS – proprietary / third party equipment
> . . . .
> LIS spreadsheet – this week's production
> . . . .
> 4. Investor meeting this week . . . shift in strategy, return to TSPU, focus on NICUS-development

8. Notes by an SEC attorney dated March 13, 2017 of a "Call with Winston Chan" state in part:

> 2/27: Anti Kohrhonen

9. Notes by an SEC attorney dated March 16, 2017 of a "Call with Wilmer" state in part:

> 2 files for 2 lab [?]
> Originally used LabDaq
> At some point in early 2013; decision made to [?]
> --T LIS – Intell. Property
> LabDaq continued in parallel of LIS from October 2013 thru middle June 2014
> Past bridge from LabDaq to LIS
> Only venous collections went into LabDaq
> Any finger stick is in LIS

Data . . . out of LabDaq file is venous
After June 2014, LIS has every record – include . . . finger v. venous
No finger stick in LabDaq @ all
LabDaq had data from demos [?]
. . . .
Can't say @ what point every tech demo is recorded in LIS
. . . .
Can try provide data in native file

--compilation of test by device
. . . .
Device "unknown" on spreadsheet?

10. Notes by an SEC attorney dated March 16, 2017 of a "Call with Wilmer Hale" state in part:

4. Do they have spreadsheets showing unique tests by device?

8. Request 13 and 14 spreadsheet
Originally used commercially available LABDAQ available system
Early 2013 – decision made to develop proprietary system
LIS, which would house data
October 2013-June 2014 – developers created abridge all data in LABDAQ in LIS
Only venous collections went into LABDAQ
All fingerstick collection in LIS
LABDAQ included pre-commercial lab data prior to Walgreens launch.
There are results that signify was conducted for demo and not lab patient
Produced only commercial testing data

*will check that can put data in excel
*will check on fingersticks prior to bridge being created

11. Government notes of a meeting with Wilmer Hale on or about May 18, 2017 state in part:

voided 10% of the tests – QA wasn't in place
. . . .
AZ AG
    reimb -- $ to patients, mostly going to Walgreens
    we reimbursed everyone
    AZ published a complaint
. . . .
thought it could take 1 month to get assays into box(?)
    thought a mere step from R&D to clinical lab
    PFM knew that 20 samples not suff.

12. Undated notes of a government call with WilmerHale attorneys state in part: “data re tests – more refined, next week, 13-15.”

13. Notes by an SEC attorney dated April 16, 2017 of a “Call with Wilmer Hale” state in part:

> “Live cycle documents – when will be produced?”
> . . . .
> Tender offer on hold. . . .

> Notes by an SEC attorney dated May 1, 2017 of a “Call with Wilmer Hale” state in part:

> $43.5 payment made today
> . . . .
> - Don’t know about company’s cash position
>
> Company will continue with tender offer and clock starts ticking once TRO has been lifted
> . . . .
> Unproduced texts . . . will review and produce only business related texts

14. Notes by an SEC attorney dated May 17, 2017 of a “Meeting with Wilmer Hale” state in part:

> 2 Future plans
> Tender offer – Wilson Sonsini – fundraising method has changed
> . . . .
> $60mm cash in hand left as of April
> $10mm burn rate per month
> --over half of burn rate is legal
> Trying to get advancement of legal fees $10-15mm
> $30mm total
>
> Walgreens – want to settle
>
> Make submissions on 5.0 through 2018
> --Need $100m to survive until 2018
> Existing investors – not sure if existing investors will put in more $
>
> --new investors
> Banks
> One-off investors –wealthy families
> --monetizing the IP
> . . . .
> IP Is valuable, not a lot of prior art
> --exploring loans secured by IP
> . . . .

> $550mm have accepted tender offer from C-1 and C-2

15. Notes by an SEC attorney dated November 29, 2017 of a "Call with Rob Khuzami" state in part:

> RK: Fortress wants to make sure no misunderstanding regarding the financing of Theranos
>
> --explain what the financing looks like
> Don't want any surprises
>
> . . . .
> Not looking to get any blessing from the SEC
>
> RKohl: We cannot give blessing
> We cannot disclose parts of investigation or where is headed
> RK: we can answer any questions about use of proceeds
>
> ES: Don't want clients to be shocked if we say nothing
> Don't want to be position where Fortress asks why we didn't warn about the transaction
>
> RK: Fully understand that we will not get blessing. Encourage us to ask questions – they want to be helpful. Believe that Tom Strickland will attend with Fortress.
>
> RKohl: Feel free to reach out to Justice and we can coordinate
> Noon looks fine for a meeting

16. Notes by an SEC attorney dated June 23, 2017 of a "Call with Wilmer Hale" state in part:

> (1) Fundraising – whether secured by assets, underwriters assisting, what timing, who leading communications, term sheet, list of poss. Investors
> . . . .
> (6) Search terms – narrow date range
> . . . .
> (9) Theranos considering a debt raise
> Putting together term sheet
>
> --seek funds from current investors, before going out
> Need bridge capital
> Convertible notes, not secured
>
> . . . .
> Offered to C-2 investors who participated in settlement.
> . . . .
> Holmes texts . . . did not include intensely personal nature may exclude personally embarrassing
> There is a concern that she is a public figure
>
> --included other private things – excluded

17. Notes by an SEC attorney dated July 5, 2017 of a "Call with Michael and Katie (Wilmer)" state in part:

> Elizabeth Holmes and David Taylor are interacting with investors.
> Company is at a critical juncture at now – will have a chilling impact on the company's survival

18. Notes by an SEC attorney dated July 20, 2017 of a "Call with Wilmer Hale" state in part:

(6) Fundraising . . . hoping to finalize Walgreens deal this week.

19. Notes by an SEC attorney dated July 28, 2017 of a "Call with Wilmer Hale" state in part:

> Theranos has not received a commitment to invest
> --has not provided term sheet to others aside from list
> Have provided the term sheet to bank
> Applied Capital – TCP Advisory
> Provided IP to Perkins Coie – no update
>
> Company projected $43mm cash on hand
> --had heard burn rate of $10mm per month
>
> Walgreens settlement . . . . .
> Plaintiffs injunction to stop Theranos from paying out class certification.

20. Notes by an SEC attorney dated August 12, 2017 of a "Call with Wilmer Hale" state in part:

> (7) Still hoping to raise more capital survive longer
> Involved in a study at UCSF regarding efficacy of assays on the TSPU
> --hoping they are on the right track
> "whatever you think of Elizabeth and company," technology is promising
> . . . .
> Trying to do what they can with $ they have

21. Notes by an SEC attorney dated August 7, 2017 of a "Call with Wilmer Hale" state in part:

> (2) $43.6mm cash position
> Plan is to raise money, IP investors – no commitments

22. Notes by an SEC attorney dated November 17, 2017 of a "Wilmer Hale Mtg" state in part:

TS . . . believe a resolution around 17(a)(3) fits the facts
. . . .
10b-5 would be devastating even if EH [?] than company
. . . .
Cooley & DWT are in a better position
--they believed they were saying when said it
--case is largely circumstantial
. . . .
Sophisticated investors . . . w/o . . . diligence
--inexperienced management is relevant to the state of mind
. . . .
Reality is the charges will be death . . . of the company
. . . .
DT . . . Fortress 100m debt facility
Targets Thanksgiving; end of month
Need to get certain shareholders [consent?]

23. Undated SEC notes state in part

$100M debt facility with Fortress
--up to date on what is going on with SEC
Targeting Thanksgiving for close – end of month
Most of largest shareholders have been told and are supportive
Madrone, Devos, PEER – largest shareholders will need to vote
Against the whole IP
--SPV that holds IP, Fortress owns it
Debt covenants are strong
--terms of loan for 3-5 years

24. Notes by an SEC attorney dated November 29, 2017 of a "Meeting w/ John Dwyer & Steve Neal" state in part:

If Fortress goes through; carries through end of 2018
. . . .
Current view is it makes company [secure?]

25. On numerous occasions, including on December 18, 2017, government attorneys had phone calls with lawyers at WilmerHale representing Theranos. During these conversations, the parties discussed Wilmer's rolling document productions made in response to outstanding grand jury subpoenas. The conversations addressed a variety of topics, including Wilmer's set of search terms, and the government's request to Wilmer to supplement its search terms.

26. Notes by an SEC attorney dated December 19, 2017 of a "Meeting with John and Steve" state in part:

SN . . . If meet Fortress plan requirements, company would be ready for an IPO in ? years

> JD . . . Board thinks EH should be at the helm today. Whether she should stay on after IPO is a question, but don't want to take that off the table.
> . . . .
> If she cannot be the CEO of Theranos after IPO, that would be taking away the option – some value to shareholders
> . . . .
> The loan that company gave her to purchase the stock
> --no money changed hands
> No ill-gotten gain
> The stock is going to be a significant issue
>
> Believe the fraud, if any, would have started 2013 with the C-2 round
> Believe that the investors were playing with play money and did not conduct adequate due diligence
> November 2013-2015 during C2 round
> . . . .
> Her ability to pay is based on her salary – contingent on company going forward
> She doesn't have a million dollars to give us now
>
> ES Need a multiple of her salary – millions

27. Notes by an SEC attorney dated February 14, 2018 of a "Call with Wilmer and Cooley" state in part:

> SE. The language is important to EH
> . . . .
> The staff isn't required to plead fraud or deceit
> Haven't seen anything to support that
> Written and oral communications
> --gap between what was said and what was heard
> Inventors were talking about potential of invention, rather than current state
> Risky and ambitious plan but investors understood risks.
> What happened with FDA – not relevant
>
> CD . . . communications with FDA don't have anything to do with investors.
>
> SE: client was young and inexperienced
> She relied on others for their experience and put in place knowledgeable advisors
> There is a stumbling on execution of business plan
> and a lack of procedures in place for a company moving forward quickly.
> -EH can live with this
> SEC can typically show self-dealing
> -no self-dealing
> Acknowledgment would go a long way
> Process and procedures are getting better
> --would be helpful to see in a complaint

> CD: We have the challenge of reconciling complaint with complaint against Balwani.
> . . . .
> SE: This is a unique case
> Have not seen misstatements that can tie to particular individual.
> Citing specific misstatements will be easier to get sign-off on
> . . . .
> CD: . . . What is important is this be described in a manner that reflects recklessness and not a scheme intended to defraud
> This is not a case where principals are keeping separate set of books.
> Ample evidence of lack of maturity, rather than desire to mislead people
> There are explanations for what was said
> . . . .
> Katie is finalizing a privilege log
> Trying to work with document certification to modify.
> SE: In the process of getting tax returns and bank statements.

17. Notes by an SEC attorney dated March 12, 2018 of a "Call with Wilmer and Cooley" state in part:

> Have proposed final edits to board
> Overreaching thematic point – complaint makes it seem like this was a Ponzi scheme
> . . . .
> Haven't tried to soften the language
> . . . .
> Draft of document at Wilmer's or Cooley's office
> . . . .
> Fraudulent scheme is stricken from the summary
> Read like no intent to develop a technology that was viable
>
> Theranos and Holmes were reckless in making these statements, often being unclear about status of technology nor did their descriptions of tech reflected current status of technology given developments to date
> . . . .
> Fortress warrant is not included in the 625 number

18. Notes by an SEC attorney dated March 13, 2018 of a "Call with Cooley and Wilmer" state in part:

> (2) Para 3 – "virtually every aspect" "many" fine
> . . . .
> Knew there was substantial cash coming in <u>no</u>
> Even if not revenue
>
> (7) Para 93 – delete 'defrauded' in front of investors. <u>No</u>

19. In advance of Wilmer's March 14, 2018 production to the government that was labeled THER-2609026 through THER-2627934, and included blood test lab reports generated via Theranos' LIS and LABDAQ systems, the government and attorneys at Wilmer discussed the fact that Wilmer would be withholding from its production certain test results, such as those that reference CD4+T-Cell test results. These telephone conversations, between Wilmer and the government, occurred over the course of several dates, on dates unknown, but likely in or around February and March 2018.

20. Notes by an SEC attorney dated March 22, 2018 of a "Call with Jeff and John" state in part:

> (2) Theranos has funding runway through the summer. IEEE evaluated IP
> portfolio and one of the top 3 companies – ½ billion dollars
> Will start laying off people soon

21. On or about April 8, 2018, the government hosted an in-person meeting at the USAO in San Jose with one or more lawyers from WilmerHale regarding Theranos. Chris Davies is believed to have been present for this meeting. The government understands that WilmerHale asked for the meeting to update the government on developments at Theranos, including the purchase of some of its intellectual property by Fortress. David Taylor was present for this meeting. At this meeting, someone, believed to be David Taylor, stated in substance that Theranos's "runway" would last until July 2018.

22. In or about April 2018, attorneys at WilmerHale asked to meet with government supervisors in the event the line prosecutors recommended charging the corporation.

23. On or about April 26, 2018, Matthew Benedetto of WilmerHale stated to the government: "the Company will be producing all lab reports held in LIS from the commencement of retail patient testing to about September 19, 2015 (when the CTNs ceased being used), including unredacted HIV test results. We will reproduce the lab reports from the period covered by the prior production to include these HIV test results."

24. On or about May 4, 2018, counsel for Mr. Balwani wrote the government:

> Thank you again for meeting with us last Friday with your team. We hope that you will agree with us that Sunny's liability for Theranos-related matters, if any, will and should be fully addressed by the civil actions, including the pending SEC enforcement case in San Jose, the Attorney General's action and pending class action lawsuit in Arizona, and the pending class action lawsuit in San Jose. As we discussed, the burden of those cases is very substantial and will fall almost entirely on Sunny's shoulders.
>
> "If any event, I wanted to let you know that we had a discovery conference with SEC counsel yesterday, and agreed that we would receive the Commission's

> initial disclosures on May 17, with the documents they obtained from third parties to follow within a reasonable time after that, subject, we are told, to the workload of their document processing department. We expect to receive this material and additional material we have requested within the next two months, or perhaps sooner. Although of course we understand that your office has conducted its own investigation, we assume that the Commission's case at least overlaps with the evidence relevant to the criminal investigation.
>
> Whether we agree on the proper course of action in this matter, there is no question that the case is highly complex, involving a great many documents and witnesses, and thus if indicted would consume substantial time and resources on both sides. Before the government commits to that process -- which regardless of outcome would dramatically alter not only Sunny's life but also the lives of his family members who look to him for support and leadership -- we think that the government as well as Sunny would benefit from a discussion of more of the specific evidence that we will receive from the SEC, and perhaps from your office if you are willing to provide any pre-charge discovery in the form of a reverse proffer or otherwise. As we discussed last Friday, we believe that even the limited number of SEC transcripts we received only a week before our meeting cast substantial doubt on the investor fraud allegations in the Commission's case, particularly regarding Sunny's intent. For this reason, we believe that the government could only benefit from further dialogue that takes into account additional evidence and such of the government's charging theories that you may be willing to share.

25. On or about May 10, 2108, counsel for Ms. Holmes wrote the Attorney for the Government stating, in substance, there were two factors why no prosecution was warranted: "virtually no evidence . . . to support a jury finding that Ms. Holmes acted with an intent to deceive" . . . and "your office has, to date, given insufficient weight to Ms. Holmes' settlement with the [SEC]."

26. On or about May 16, 2018, counsel for the government wrote WilmerHale as follows:

> Hi Wilmer folks,
>
> Can we have a call today or tomorrow to talk about a few outstanding items on the to-do list? So you can have the right people on the call, here are the topics we'd like to discuss:
>
> - Timing of production of 2016 and 2017 documents, and Theranos's proposed privilege filter
> - Production of additional items requested in subpoena served on April 20, i.e., lab data, exemplar devices, and materials re advertising / marketing
> - Updates regarding Brad Arington's knowledge of a false statement made by Holmes to the FDA / CMS

> Jeff and I are available toward the end of the day today and generally available tomorrow, so please let me know what times might work for you.

27. On or about May 30, 2018, attorneys from WilmerHale stated to attorneys for the government: "Would you guys have time for a brief conversation today with Tom and me (and perhaps David Taylor as well). We'd like to catch up with you on the status of the Company's sales efforts."

28. Shortly before on or about June 1, 2018, the government had a call with several attorneys at Wilmer (representing the company) and the Theranos GC. It was said that Theranos was in the process of looking for a buyer for its assets (mainly IP). There were several upcoming dates that were allegedly important to the sale process. Those dates were June 15, July 15, and August 15. It was requested that the government not indict anything or anyone, but if it did, it was requested that the government delay indictment until after August 15. If that was not doable, it was requested that the government consider delaying until after July 15, or even June 15. It was said that each "fifteenth" that passed without additional negative publicity would make a sale more likely. It was also claimed that a sale was the only way investors would see ROI.

29. Notes by an SEC attorney dated June 18, 2018 of a "Call with Michael Mugmon" state in part:

> Joint defense agreements
> PFM depo videos
> Colman depo transcripts/videos
> Website captures
> QAD preservation
>
> Extremely low on cash and people
> QAD has been preserved / website preserved

30. On or about July 23, 2018, an attorney of a law firm representing individuals interviewed by the government stated that the attorney "wanted . . . make sure you [i.e., the government] were aware of the . . . sales of Theranos assets." The attorney noted "[w]e have heard rumors that this was done in a manner specifically to avoid the use of the Theranos name." The attorney referred the government to the following website:

https://www.bidspotter.com/en-gb/auction-catalogues/bschilc/catalogue-id-bschilc10084

31. On or about July 25, 2018, an AUSA wrote several attorneys at WilmerHale as follows:

> Wilmer team,
>
> Thanks again for taking the time to speak to me the other day. I wanted to follow up on the topics we discussed to make sure we're on track to wrap everything up

in the next couple weeks. In particular, I thought it would be helpful to set some compliance deadlines as laid out below.

Production of Devices

Thanks for providing the description of the devices in Theranos's possession. If you'd like us to consider postponing our request for a given model on the grounds that the company only has one copy and needs access to it in the short term, please identify which models that applies to and briefly explain the need for the company to retain possession. Please provide this information by Monday, July 30. As to any unique devices we don't get in this round, the government would expect Theranos to maintain them in the company's possession without altering them or relinquishing custody to any other parties. Speaking of which, I've looked into your question regarding the anticipated request from Holmes and Balwani for those same devices. I've found no support for the proposition that a party is excused from complying with a grand jury subpoena on the basis of a competing request from a defendant—especially where the grand jury subpoena was served first and the Rule 17 subpoena has not been issued. It's routine, of course, for the government to take possession of unique evidence items relevant to a criminal prosecution. Defendants have a right to inspect such evidence seized by the government, but they don't have the power to deprive the government of that evidence by making competing requests. Please let me know if you have any authority to the contrary. Based on our understanding of the law, we don't think it would be appropriate for Theranos to delay production to the government based on a conversation it had with defense counsel.

The deadline for compliance with the request for devices is <u>August 8, 2018</u>. Please deliver the requested devices to the FBI or have them ready for pickup by that date. As a reminder, that subpoena request also included samples of other proprietary devices including the sample collection device and nanotainer.

Remaining Documents & Privilege Filter Issues

On the topic of 2016-2017 docs, we've received one production and understand you are preparing an additional production. The additional production will include, among other things, communications with non-lawyer third parties that were withheld based on your initial privilege filter. Please also include in that production any non-privileged documents to, from, or mentioning Heather King. Given her expansive role at the company and her involvement in relevant events, we can't accept a production that simply excludes anything with her name on it. We are fine, however, with Theranos keeping Scott Marmer's name on the privilege filter, based on your representations that his role was mainly limited to contracts and IP and the fact that any communications between him and non-lawyers outside of Theranos will be captured and produced as discussed above.

> The deadline for compliance with this document request is August 20, 2018. Please let us know by August 8 if Theranos won't comply so that we can determine next steps.
>
> **LIS Database + Software**
>
> I understand from our conversation that you've received the LIS database from Theranos and are preparing it for production to us next week. To comply with the subpoena, please complete that production—including any software necessary to access and query the database—by August 10, 2018.
>
> Please feel free to reach out by email or phone if you'd like to discuss any of the above.

32. On or about July 30, 2018, an attorney with WilmerHale wrote the government:

Thank you for speaking with us, we very much appreciate your time. Pursuant to our conversation last week, we wanted to circle back on the open items discussed on our call and in your email below.

Production of Devices

At this time, Theranos would appreciate postponing the requests for certain devices identified below. Currently, only a single copy of each of these device versions exists, and the Company hopes to retain these unique devices so that it can demonstrate the evolution of its technologies to potential buyers or other potential partners.

- Theranos Bench Prototype
- Theranos Monolab
- Theranos Minilab 4.1-TC

Additionally, it appears that two miniLab 4.1 devices were incorrectly identified as the previous miniLab 4S versions. As such, the Company will not be able to provide a version of the miniLab 4S, as most of these devices were disassembled and reused to build the miniLab 4.1 in 2015 and early 2016. The Company is working to prepare its devices for transport and is happy to have these devices ready for pickup before August 8th (if possible, we believe scheduling a pickup for Monday, August 6th would work well on our end). As we have discussed, we would appreciate it if this pickup could be handled with discretion. We will provide you with a list of the devices we will have ready for pickup, and are of course happy to work with you and/or the FBI to arrange for the pickup of these devices. Please don't hesitate to let us know if you have any other questions on this front.

Remaining Documents & Privilege Filter Issues

We are continuing to discuss this issue with our client and hope to get back to you shortly. We will circle back by August 8th to let you know our preferred option(s) on this front and to discuss next steps.

LIS Database + Software

We are working with the Company to prepare the LIS database for production. We have also been in touch regarding your request for additional information on any proprietary software necessary to query the LIS database, and are working with the Company to better understand this issue. Thus far, we have determined that the following software/operating system(s) will be necessary to restore and query the database:

- Microsoft SQL Server Enterprise License on Windows Server 2012R2
- SQL Server Management Studio 2014 Management Studio or any other standard software to query SQL Server database

Because the above software/operating system(s) are technically the property of third parties, we feel it is appropriate for you to obtain access via the relevant third parties. We are of course happy to work with you and provide any other information to assist you in this regard.

Thank you again for your time, and please don't hesitate to let us know if you have any questions or would like to discuss any of the above. We will of course circle back on these open items per your email below.

33. On or about August 7, 2018, an attorney for WilmerHale wrote the government:

We are prepared to turn over the devices listed below. As we've discussed previously, these are the devices for which Theranos has more than one copy. I also included packaging dimensions and item weights so you can coordinate appropriate sized vehicle and resources for loading. There will be total of six (6) packages for pickup.

Please let us know when the agent or agents will be available to pick up the devices. We have a preference for 2pm on Wednesday, August 8th, but if that time does not work on your end we can find another time that works.

<u>**Testing Devices**</u>

- Edison 3.5 (only THE-manufactured device used in clinical lab) -> ***Edison35_40-01006_06AUG2018.jpg (14"-W x 20"-L x 20"-H, Weight ~40lbs)***
- miniLab Tower -> ***miniLab-Tower_40-01000_06AUG2018.jpg (Pallet 28"-W x 67"-L x 28"-H, Weight ~300lbs)***
- miniLab 4.1-Full -> ***CASE_T41-C010_miniLab41-FULL_40-01016_06AUG2018.jpg (Case 28"-W x 32"-L x 26"-H, Weight ~130lbs)***

> - miniLab 4.1-Lite (version used for UCSF study) -> **CASE_T41-C033_miniLab41-LITE_40-01019_06AUG2018.*jpg* (Case 28"-W x 32"-L x 26"-H, Weight ~110lbs)**
> - miniLab 4.1-TC V2 (current version, used in R&D for Zika) -> **CASE_T41-C023_miniLab41-TCv2_40-01024_06AUG2018.*jpg* (Case 28"-W x 32"-L x 26"-H, Weight ~120lbs)**
>
> **<u>Collection Devices & Cartridges -></u>**
> ***Packed_TSCD&Cartridges_06AUG2018.jpg (small box, content pictures included for reference as described below)***
> - TSCD -2 (LiHep) -> ***TSCD2_50-00120_LiHEP_06AUG2018.jpg***
> - TSCD -2 (EDTA) -> ***TSCD2_50-00121_EDTA_06AUG2018.jpg***
> - Zika, fully assembled, with reagents (recent R&D use) -> ***Cartridge_60-00186_06AUG2018.jpg***
> - Training cartridges, fully assembled -> ***Cartridge_60-00187_06AUG2018.jpg***
>
> At this time, Theranos will not be providing the devices listed below because it only possesses one copy of each. You will note the addition of two cartridges to this list.
>
> - Theranos Bench Prototype
> - Theranos Monolab
> - Theranos Minilab 4.1-TC
> - HSV-2 IgG Assay Cartridge
> - Custom Potassium Cartridge
>
> Please let me know if you would like to discuss or if there is a particular agent or agents with whom we should be coordinating.

The attorney attached photos of the referenced devices.

34. On or about August 27, 2018, Katie Moran wrote government attorneys: "Attached please find the transmittal letter accompanying today's production of Theranos' LIS database. The media will be delivered via courier today. The encryption key is 7Dh$fsB!dgs&6Fes!." On August 29, 2018, a government attorney replied: "We've received that production—thank you. Please provide a status update on Theranos's plans regarding the outstanding 2016-2017 documents at your earliest opportunity. In order for us to determine appropriate next steps, it would be helpful for us to have a clear statement of the company's intentions with respect to complying with the subpoena. Separately, we discussed obtaining the deposition transcripts from the Colman litigation. I understand that under the protective order you needed to provide notice to certain parties. Has that issue been resolved such that you can send us the transcripts today?" On or about September 4, 2018, Michael Mugmon wrote attorneys for the government: "I understand that Katie has been in touch with you to advise you that Theranos intends to make a fully responsive production next week, upon consideration of John's email below. Am I correct that you nonetheless intend to file a motion to compel (which I assume would make clear that DOJ is seeking, among other things, non-privileged

communications from lawyer custodians), notwithstanding that (1) you will shortly be getting everything you asked for (and more); and (2) John's email made quite clear that we were to contact you before COB today if we wanted to avoid motion practice (which we do)? I'm not sure what would be the relief seek in your motion, if you do intend to file one. And I'd personally find it disappointing if you do intend to file a motion where we were given time to and did consider your position — and are giving you what you've requested. I assume that you would not be using this motion to cast the Company in a negative light to support your indictments. I am taking time away from my vacation out of the country to respond to this, and I would hope that we could have your professional courtesy."

35. On or about September 4, 2018, Michael Mugmon wrote to attorneys for the government: "I now understand that it is Mr. Balwani's counsel that intends to file a motion to quash the subpoena. If that is not correct, please let us know. If, however, the below is right, we would like to continue meeting and conferring." An attorney for the government replied: "Thanks for reaching out. I think your first email was based on a misunderstanding and that you have things straight now. The sole purpose of a motion to compel would be to obtain the documents covered by the subpoena. If Theranos is going to produce those documents pursuant to the subpoena and without the need for further court order, there's no need for any such motion. I understand from speaking to Katie a few minutes ago that Theranos is processing the production now and that we'll get it as soon as it is ready next week. I also understand that Theranos intends to produce those documents regardless of any motion that Mr. Balwani's lawyers might file in the criminal case. If that's correct, I expect that the issue I raised in my September 1 email will be resolved with that production. Please let me know if I'm misinformed about the company's plans. Thanks again for taking the time to write. I appreciate your attention to the matter and hope you enjoy the rest of your vacation."

36. Shortly after receiving an encrypted hard drive with what was purported to be "a copy of Theranos' LIS database" on or about August 27, 2018, FBI Agent Scussel, at the direction of an attorney for the government, sent the encrypted drive by Federal Express to a paralegal in the USAO.

37. On or about September 5, 2018, a USPIS representative not connected to the investigation forwarded to Chris McCollow a newspaper article to the effect that Theranos was shutting down.

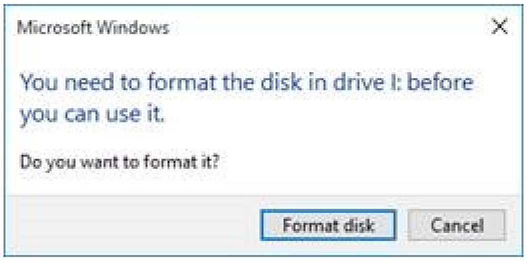
38. On or about September 12, 2018, Katie Moran from WilmerHale stated to the government that the company was probably dissolving that day and that WilmerHale would not be able to act for the company after that. Moran indicated WilmerHale was still planning to produce a final batch of documents to the government at the end of the week. She also provided the name of the assignee and the law firm representing the assignee.

39. On or about September 12, 2018, a paralegal in the USAO reported to an Automated Litigation Support (ALS) supervisor with the USAO that she had two hard drives in her possession. The paralegal indicated she had wanted to send one of the hard drives to the ALS supervisor, that is was a 1 TB drive but that she was not sure what the data size was; her computer was not detecting the data size. The paralegal planned on sending the hard drive to the IT department of the USAO to take a look. If the IT department was able to fix it, the paralegal

planned to have the IT department give it to the ALS supervisor. The paralegal indicated if the IT department was able to fix it, she would execute routine ALS forms to provide details on what the paralegal wanted done.

40. Later on or about September 12, 2018, the ALS supervisor agreed to the paralegal's plan and offered to look at the drive as well, noting ALS had its little tricks to try and coax drives to play nice. The paralegal advised that after a call with an IT department representative the paralegal decided to send the drive directly to ALS for processing.

41. On or about September 14, 2018, the ALS supervisor advised the paralegal, an IT department representative, and a USAO employee in the ALS unit that she had received the drive that afternoon but it was not playing nice for her either. She reported receiving the following message on both her workstation and a standalone computer:



You need to format the disk in drive I: before you can use it.

Do you want to format it?

The ALS supervisor initially guessed that that the drive might be formatted for a Mac or simply corrupted. She discussed the matter with an IT department supervisor and the USAO employee in the ALS unit, who wondered whether the entire drive might be encrypted as a VeraCrypt (or TrueCrypt) volume. The ALS supervisor noted that if that were the case, the ALS unit would need a password to unlock it. She asked whether the originator of the drive provided any documentation as to the contents and/or a password? She provided a scan of the drive label to assist in tracking down a password.

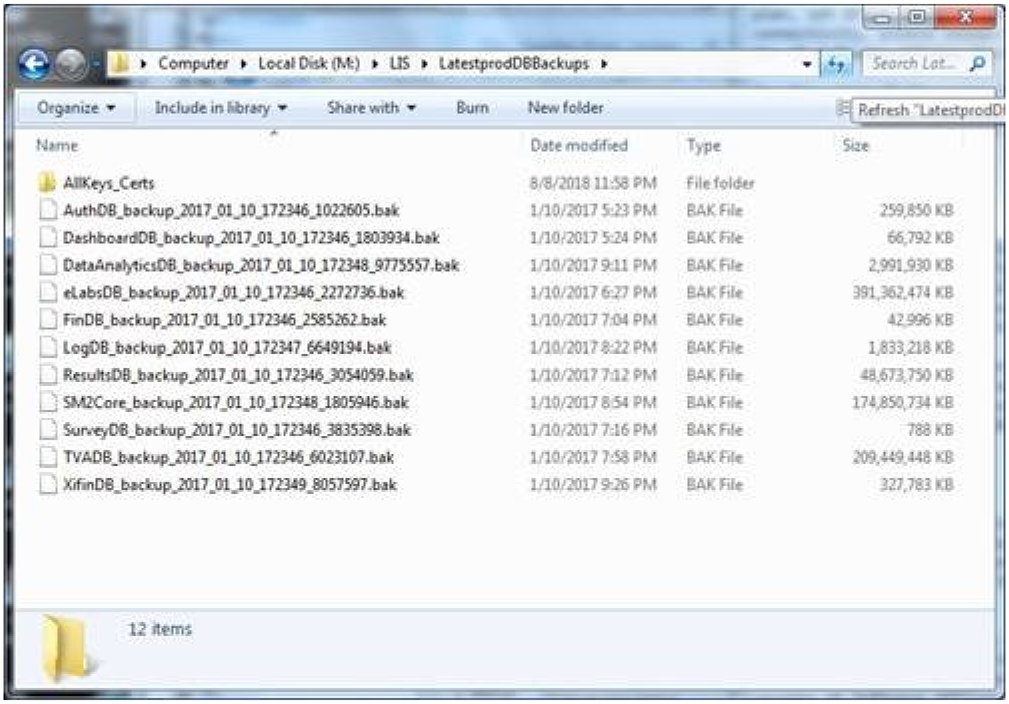
42. On or about September 15, 2018, the paralegal reported to the ALS supervisor, the IT department representative, and the USAO employee in the ALS unit that she had found the hard drive is password protected and provided the following password: 7Dh$fsB!dgs&6Fes!

43. On or about September 18, 2018, the ALS supervisor advised the paralegal and the USAO employee in the ALS unit as follows:

> It looks like [the USAO employee in the ALS unit's] diagnosis was correct; we couldn't see the contents of the drive because it's a VeraCrypt volume (a drive which has been encrypted using VeraCrypt).
>
> Using the password you provided I was able to open it on the standalone, but now I just have further questions!
>
> The contents of the drive *do not* appear to be load ready files, or natives, or any kind of forensic viewer. Rather, It looks like a set of backup copies of something, probably a database (the format is .bak).

> Without knowing what sort of database these are from (or if they indeed are database backups) it's very hard to figure out how we might extract the data (or even if it's possible for us to do so).
>
> It also raised the question that perhaps these are simply backup copies of material that has already been provided to our office.
>
> Was there any documentation provided when the drive was delivered?
>
> If you could send along any additional info you have about this drive that would be great; I'm also happy to speak with an agent if you have a point of contact for this material.

The ALS supervisor also provided the following screenshot:



Name	Date modified	Type	Size
AllKeys_Certs	8/8/2018 11:58 PM	File folder	
AuthDB_backup_2017_01_10_172346_1022605.bak	1/10/2017 5:23 PM	BAK File	259,850 KB
DashboardDB_backup_2017_01_10_172346_1803934.bak	1/10/2017 5:24 PM	BAK File	66,792 KB
DataAnalyticsDB_backup_2017_01_10_172348_9775557.bak	1/10/2017 9:11 PM	BAK File	2,991,930 KB
eLabsDB_backup_2017_01_10_172346_2272736.bak	1/10/2017 6:27 PM	BAK File	391,362,474 KB
FinDB_backup_2017_01_10_172346_2585262.bak	1/10/2017 7:04 PM	BAK File	42,996 KB
LogDB_backup_2017_01_10_172347_6649194.bak	1/10/2017 8:22 PM	BAK File	1,833,218 KB
ResultsDB_backup_2017_01_10_172346_3054059.bak	1/10/2017 7:12 PM	BAK File	48,673,750 KB
SM2Core_backup_2017_01_10_172348_1805946.bak	1/10/2017 8:54 PM	BAK File	174,850,734 KB
SurveyDB_backup_2017_01_10_172346_3835398.bak	1/10/2017 7:16 PM	BAK File	788 KB
TVADB_backup_2017_01_10_172346_6023107.bak	1/10/2017 7:58 PM	BAK File	209,449,448 KB
XifinDB_backup_2017_01_10_172349_8057597.bak	1/10/2017 9:26 PM	BAK File	327,783 KB

12 items

44. On or about September 20, 2018, the government spoke with attorneys from Dorsey representing the Assignee. The call participants discussed state law governing assignments for the benefit of creditors, the contract governing the assignment, board and shareholder approval, Fortress, and the Assignee's approach to privilege.

45. On or about October 4, 2018, the government paralegal advised the ALS supervisor (and attorneys for the government) of an upcoming vacation through October 19, 2018, and inquired whether she was able to find the program that would enable the government to view the hard drive (described above).

46. On or about October 5, 2018, the ALS supervisor advised attorneys for the government and the government paralegal about issues surrounding the hard drive. She noted she had discussions with her unit, the IT department, and the LTSC. She said the drive does not contain material which could be processed in house or by the LTSC. She said the drive contains 12 BAK files totaling about 830 gigabytes. She said the .bak extension indicates that the files were most likely backup files for a Microsoft SQL database. She said if that was correct such files would be used to restore database backups on a Microsoft SQL Server. She said .bak is a common extension and without documentation of what the drive was meant to contain she could only make an educated guess that these were database backups. She said because they were archive files the size of the data could increase when restored. She said the material was not provided to the USAO in a format that can be extracted, viewed, or processed by available software. She said the LTSC's EDD [electronic data discovery] software can only digest SQL.bak files if they are under 300 mb. She suggested a possible route forward of pushing the producing party to see if the party could be persuaded to produce in a manner that can be viewed and processed in a standard way rather than an unspecified archive format the government could not access. She suggested encouraging the producing party to consider handing over its physical SQL server and setting it up in a workroom. She suggested checking with the FBI or other agencies to see if they have resources that can process large SQL database archives. She suggested identifying a vendor who could process the material and noted the data size and labor cost could be staggering. She offered to set up a call or meeting to discuss the issues further.

47. On or about October 30, 2018, the government paralegal advised the ALS supervisor she had met with attorneys for the government and the group decided to pursue the options of pushing the producing party to see if it could be persuaded to produce in a manner that can be viewed and processed in a standard way rather than an unspecified archive format the government could not access and checking with the FBI or other agencies to see if they have resources that can process large SQL database archives. The government paralegal also advised the ALS supervisor to return the hard drive when she had a chance. Around that time, the ALS supervisor did so. The hard drive remained in the possession of the government paralegal until around the spring of 2020.

48. In approximately October and November of 2020, counsel for the government was in contact with counsel for the assignee at the Dorsey law firm on a variety of topics. During those discussions, government counsel noted that the government had been unable to access the copy of the LIS database produced by Theranos. Assignee counsel expressed a lack of surprise that the government was having difficulty accessing the database, and offered to investigate whether the assignee had the database in a different form that would facilitate the government's access. During a subsequent conversation, assignee counsel reported back to the government that it had been unable to locate an alternative version of the LIS database that would allow access. Assignee counsel also informed government counsel that the LIS database was encrypted and that the assignee lacked the means to decrypt it. Assignee counsel opined that Sunny Balwani would likely be able to decrypt the database, but could not identify anyone else who they thought could accomplish the task.

49. On or about January 14, 2019, the government paralegal advised attorneys for the government that ALS had tried to process the hard drive but does not have the software to process the discovery and proposed possible options of producing a native version, involving the

FBI computer forensics team, involving a third party, and/or reaching out to the source. On or about January 29, 2019, the government paralegal provided a similar update.

50. In March of 2019, government counsel contacted assignee counsel to ask some follow-up questions about how the LIS database came to be encrypted and decommissioned. On March 21, 2019, assignee counsel emailed an attorney for the government and conveyed the assignee's understanding that Sunny Balwani and Shekar Chandrasekaran encrypted the LIS database. In that email, assignee counsel also quoted David Taylor, former Theranos president, as stating that the LIS database was "the most comprehensive (though still not fully comprehensive) company repository of clinical information -- patient contact info, doctor contact info, test dates and results, etc. It has, however, been decommissioned, and before the company formally closed we were advised that it be a herculean undertaking to get it up and running again." Assignee counsel promised to speak to the assignee to determine whether they had any additional information.

51. On March 25, 2019, assignee counsel followed up with an attorney for the government and passed along information from Jarod Wada at the assignee entity. Wada confirmed that the assignee did not know who decommissioned the LIS database. Wada also conveyed that Eric Caddenhead, former IT manager of Theranos heard that Shakar Chandrasekaran had been involved with the LIS database, and that Caddenhead had stated that the LIS database was maintained by a group outside of Theranos, Inc. That email also conveyed that David Taylor had told Wada on several occasions "that the LIS was decommissioned and that prior to ABC, Theranos, Inc. had been told that it could no longer be reconstructed with the existing resources." The assignee also reported that a company called FTI Consulting had done some work via WilmerHale on behalf of Theranos, and relayed from a representative of that company that FTI had not decommissioned the database.

52. In or about March or April of 2020, an attorney for the government called WilmerHale attorney Matthew Benedetto and/or Michael Mugmon. The purpose of that call was to inquire as to whether WilmerHale was in possession of additional passwords or other information that would allow the government to access the purported copy of the LIS database that had previously been produced by WilmerHale when it represented Theranos. During that call or a follow-on call, the attorney(s) from WilmerHale confirmed that they did not have any such additional information beyond what they had provided earlier.

53. In or about May 2020, Special Agent Scussel retrieved an encrypted hard drive from the USAO and took it to the FBI's RCFL.

54. In or about June 2020, Special Agent Scussel retrieved an encrypted hard drive from the RCFL, returned it the grand jury file, and provided four copies to the USAO.

Very truly yours,

STEPHANIE M. HINDS
Attorney for the United States,
Acting Under Authority Conferred
By 28 U.S.C. § 515

/s Robert S. Leach

ROBERT S. LEACH
JEFFREY SCHENK
JOHN C. BOSTIC
VANESSA BAEHR-JONES
Assistant United States Attorneys

cc Jeff Coopersmith, Esq. (by email)

EXHIBIT D

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

PARTNER INVESTMENTS, L.P., a
Delaware limited partnership,
PFM HEALTHCARE MASTER FUND,
L.P., A Cayman Islands limited
partnership, and
PFM HEALTHCARE PRINCIPALS
FUND, L.P., a Delaware limited
partnership,

Plaintiffs,

v.

THERANOS, INC., a Delaware
corporation, ELIZABETH HOLMES,
an individual, and RAMESH BALWANI,
an individual, and DOES 1-10

Defendants.

C.A. No. 12816-VCL

DEFENDANT THERANOS, INC.'S RESPONSES AND OBJECTIONS TO PLAINTIFFS' FIRST SET OF INTERROGATORIES

Pursuant to Court of Chancery Rules 26 and 33, Defendant Theranos, Inc. ("Theranos" or the "Company") hereby submits the following responses and objections to Plaintiffs' First Set of Interrogatories (each an "Interrogatory" and, collectively, the "Interrogatories") as follows:

GENERAL OBJECTIONS

Theranos makes the following General Objections to the Interrogatories and incorporates them by reference into its response to each Interrogatory below as though fully set forth therein.

> REQUEST NO. 54: DESCRIBE the "proprietary databases" to which YOU referred in YOUR response to Interrogatory Nos. 18, 19, 21, 33, 28, and 29, including the contents, all available data points, date ranges for available data, data sources, data collection methods, data output capabilities, compilation report capabilities, search capabilities, database administrator(s), authorized user(s), security protocols, and metadata or user tracking capabilities.

RESPONSE TO INTERROGATORY NO 54:

Theranos incorporates by reference the General Objections set forth above. Theranos specifically objects to the phrases "contents, all available data points, date ranges for available data, data sources, data collection methods, data output capabilities, compilation report capabilities, search capabilities, database administrator(s), authorized user(s), security protocols, and metadata or user tracking capabilities" as overly broad and unduly burdensome because they comprise multiple subparts.

Subject to and without waiving the foregoing objections and General Objections, Theranos states that the Theranos LIS System ("TLIS") is a proprietary application that was designed to record, manage, and store data, as well as drive workflow and aid processes, in Theranos' CLIA-certified laboratories. The database that underlies TLIS contains information pertaining to patient encounters and the laboratory test results obtained in relation to those encounters.

Database records

TLIS provides a function to define, create, and edit database records. Such records may be created via the LIS Application or other laboratory applications connected to the LIS database. TLIS provides a function to receive or retrieve each record via standard communication protocols. The following is a list of all records: Patient record, physician record, provider record, provider location record, laboratory record, lab order record, lab test record, lab visit record, container barcode record, reference range, and case. A variety of fields may be populated for each record.

Date ranges for available data

The records in the database underlying TLIS span from approximately September 13, 2013 to approximately October 6, 2016.

Data sources

Data sources include the following:

1. Automated entry of data from third-party clinical analyzers.

2. Automated entry of data from proprietary analyzers.

3. Automated entry of data from third-party Electronic Medical Record vendors via electronic interfaces.

4. Manual entry of data through the user interface.

5. Manual entry of data from third-party clinical analyzers.

6. Manual entry of data from proprietary analyzers.

7. Manual entry of data from third-party reference laboratories.

8. Manual entry of data from other sources, including client communications and the internet.

Data collection methods

Data can be collected via electronic interfaces to analyzers and third-party software vendors. Data can also be collected manually via input through the user interface.

Data output capabilities

Data output from TLIS was available through the follow capacities:

1. Export to local machine/network

2. Fax

3. Email

4. Electronic interface to third-party software vendor

Compilation report capabilities

TLIS provides a variety of template reports for users to download and export. The database may also be queried to generate custom reports for which there are not defined templates.

Search capabilities

TLIS provides functions for users to search for patient records, physician records, provider records, provider location records, lab order records, lab visit records, container barcode record, reference ranges, and cases. The database may also be queried if the user interface does not provide the desired search functionality.

Database administrator(s)

The following individuals served as database administrators:

Name	Title	Description of Role
Shekar Chandrasekaran	Head of Software Development	Mr. Chandrasekaran was a member of the Software Development team and was responsible for designing and implementing TLIS.
Sekhar Variam	Director of Engineering	Mr. Variam was a member of the Software Development team and was responsible for designing and implementing TLIS.
Arunkumar Chockaiyan	Database Architect	Mr. Chockaiyan was a member of the Software Development team and was responsible for designing and implementing TLIS.

Authorized Users

More than 200 individuals within the CLIA-certified laboratories, Product, Software Engineering, IT, and Billing teams were granted access to the LIS application, with user roles defined for various functions. To list and provide a description of all individuals who were ever granted access to TLIS, without reasonable limitation as to the significance of their roles within the Company or their relation to PFM's investment or this litigation, would be unduly burdensome and would require information that is irrelevant and immaterial to the claims or defenses of any party in this litigation. Theranos therefore provides below a list of authorized users among the document custodians in this litigation.

Theranos states that it is currently aware that the following Theranos document custodians were granted access to TLIS:

1. Hoda Alamdar
2. Brad Arington
3. Sunny Balwani
4. Max Fosque
5. Christian Holmes
6. Mark Pandori
7. Chinmay Pangarkar
8. Adam Rosendorff

9. Suraj Saksena

10. Don Tschirhart

11. Daniel Young

Security protocols

TLIS has a multi-level security implementation:

1. TLIS utilizes a central, role-based authentication system in which access is limited to a defined set of users.

2. Role-based authentication provides the ability to assign a set of privileges to a given user, limiting the set of information available to that user.

3. A complete audit trail of all changes made to laboratory results is maintained.

4. A complete audit trail of all users who viewed a given patient result is maintained.

5. Users may not delete records from TLIS.

Metadata or user tracking capabilities

Key user actions, including the viewing, entry, and release of patient laboratory results, are recorded by TLIS.

EXHIBIT E

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/07/2020

ERIC CADDENHEAD (CADDENHEAD), telephone number [redacted], email address [redacted], was interviewed via telephone. Also present for the interview were Assistant United States Attorney (AUSA) John Bostic and AUSA Vanessa Baehr-Jones. Prior to the interview, AUSA Baehr-Jones advised CADDENHEAD it was illegal to lie to a Federal Officer (Title 18 U.S.C. 1001) and CADDENHEAD confirmed he understood. After being advised of the identity of the interviewing parties and the nature of the interview, CADDENHEAD provided the following information:

CADDENHEAD has worked in Information Technology (IT) for approximately 30 years starting his first IT job at Komag in 1991. Prior to Komag, CADDENHEAD worked as a Computer Technician. Throughout his career CADDENHEAD has focused on the IT Infrastructure and Operations side of IT. CADDENHEAD started working at Theranos in May 2013 after he was contacted by a recruiter as Theranos needed someone to expand their corporate network. CADDENHEAD had been working at Fox Head Inc., but was let go when the company moved their headquarters from Milpitas, California to Irvine, California as he did not want to move. CADDENHEAD had three job titles at Theranos, but essentially did the same job throughout his time at the company which included the buildout of data centers and their maintenance. CADDENHEAD's first job title at Theranos was IT Architect. Then in March 2017 Theranos terminated CADDENHEAD when things were going badly for the company. Theranos then received additional funding and re-hired CADDENHEAD as Principal Information Systems Engineer. When he was re-hired, CADDENHEAD was responsible for the disassembly and liquidation of Theranos' corporate network. Accordingly, when CADDENHEAD first started he was responsible for building up Theranos' network, then for network operations, and at the end he was responsible for taking it down.

CADDENHEAD was the infrastructure architect for the Laboratory information System (LIS) server. The main server for LIS was off the shelf

Investigation on 04/16/2020 at San Francisco, California, United States (Phone)

File # 318A-SF-7315857 Date drafted 04/17/2020

by Mario C. Scussel

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

IT server equipment manufactured by CISCO. ANTTI KORHONEN (KORHONEN), another Theranos employee, loaded the software on the server, but did not create the software. The software for LIS was created by a group of internal contractors from IncRev Corporation. The IncRev team was lead by SHEKAR CHANDRASEKARAN (CHANDRASEKARAN), and reported to SUNNY BALWANI (BALWANI). The software group was siloed from other Theranos employees.

CADDENHEAD was surprised when he learned the software team for LIS were contractors, because of the intense security at Theranos. When CADDENHEAD first started he could only use a particular entrance and could only access certain areas, until his supervisor complained that he could not do his job without getting access to the areas he needed to get access to.

KORHONEN started working at Theranos before CADDENHEAD and was the only one left in IT during the time between when CADDENHEAD was terminated then rehired by Theranos. KORHONEN said he could not do everything by himself which caused Theranos to rehire CADDENHEAD. CADDENHEAD provided KORHONEN's cell phone number which was [redacted].

The LIS was a completely separate network which was connected to the Internet, but encrypted by a software based encryption key. Access to LIS was very restricted and one would have to go to the data center in Newark, California where LIS was housed, in order to access it. Accordingly, CADDENHEAD did not think ELIZABETH HOLMES (HOLMES) or BALWANI would have access to LIS from their desktop. In order to access the data center one would need to get a key which was controlled by Theranos Security, then as one entered the data center a camera would take your picture as you entered. Other than the photograph taken of the user upon entry, there was not a sign-in sheet or any biometrics required to access the LIS data center. CADDENHEAD never accessed the LIS database so he did not know if the system required each user to have a log-in to access the system. KORHONEN had access to LIS.

CADDENHEAD never saw HOLMES or BALWANI in the LIS room. When CADDENHEAD spoke with HOLMES about the LIS she did not seem to even know where the room was. Accordingly CADDENHEAD doubts HOLMES would have ever accessed it herself. HOLMES probably would have gone through the software group in order to access the LIS as they were also responsible for maintenance of LIS.

When CADDENHEAD left Theranos in June 2018, LIS was still up and running. CADDENHEAD had been working on removing equipment from Theranos' laboratories to include access posts and Personal Computers (PC's). Theranos employees were given the opportunity to purchase their computers when they left, but without the hard drive. The hard drives were kept for a legal hold.

After CADDENHEAD left Theranos, they hired Neetek to move the LIS to a data center in Sunnyvale, California. Neetek employee, MICHAEL CHUNG (CHUNG), telephone number [redacted], would call CADDENHEAD with questions about LIS because he did not have anyone to help him with this process. CHUNG also asked CADDENHEAD if he could help move LIS to the data center. During one call in approximately August 2018, CADDENHEAD told CHUNG that if they took the LIS apart they would not be able to access it again because then the encryption key would be lost. The encryption key was located on a disk array which had a lot of pieces and when they took the disk array apart it would have destroyed the encryption key.

JOHN MCCHESNEY (MCCHESNEY) was overseeing the shutdown of Theranos' Newark facility, which included the movement of the LIS for Theranos. CHUNG told CADDENHEAD that MCCHESNEY had advised CHUNG to remove the disks from the disk array. Accordingly the disk array was taken apart when the LIS was moved.

On April 17, 2020 CADDENHEAD provided the following additional information via email:

IncRev Corporation, 1877 Austin Avenue, Los Altos, California 94024, email address [redacted], website www.increvcorp.com, telephone number [redacted].

Others on the IncRev software development team included SEKHAR VARIAM, and SIVA DEVABAKTHINI, email address [redacted].

JOHN MCCHESNEY was the Senior Vice President of Operations at Theranos, email address [redacted].

CADDENHEAD's email will be maintained digitally in the 1A section of the case file.

EXHIBIT F

References

https://www.simple-talk.com/sql/database-administration/encrypting-your-sql-server-2012-alwayson-availability-databases/

http://blogs.msdn.com/b/alwaysonpro/archive/2015/01/07/how-to-add-a-tde-encrypted-database-to-an-availability-group.aspx

Whether you are creating a new AAG, or you are needing to add a database that has been encrypted using TDE, there are steps that you need to complete on your SQL Server 2012 Always On Primary Replica. These are:

- Create a Master Key on the Primary Replica
- Backup the Master Key
- Create a Certificate protected by the Master Key
- Backup the Certificate
- Create a Database Encryption Key
- Enable a TDE on a Database

Step by Step Process to encrypt a database in SQL Server 2012:

Encrypt Primary SQL Server with Encryption Key and Certificate:

```
USE MASTER
GO
-- Create a Master Key
CREATE MASTER KEY ENCRYPTION BY Password = 'P@ssw0rd1!7#';

-- Backup the Master Key
BACKUP MASTER KEY
   TO FILE = N'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\Certs\MyMasterkeyFile'
   ENCRYPTION BY Password = 'EncRyption#1$';

-- Create Certificate Protected by Master Key
CREATE Certificate MyServer_Cert
  WITH Subject = 'My DEK Certificate';

-- Backup the Certificate
BACKUP Certificate MyServer_Cert
   TO FILE = N'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\Certs\MyServer_Cer.Cer'
   WITH Private KEY (
       FILE = N'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\Certs\MyServer_PrivKey.pfx',
       ENCRYPTION BY Password = 'RestoRe%23'
   );
```

Encrypt the databases on primary SQL Server:

Encrypt ELabs DB:

```
-- Move to the database you wish to enable TDE on
USE elabsdb
GO

-- Create a Database Encryption Key
CREATE DATABASE ENCRYPTION KEY
  WITH Algorithm = AES_128
  ENCRYPTION BY Server Certificate MyServer_Cert;
-- Enable the Database for Encryption by TDE
ALTER DATABASE elabsDB
  SET ENCRYPTION ON;
```

Encrypt Auth DB:

```
-- Move to the database you wish to enable TDE on
USE AuthDB
GO
-- Create a Database Encryption Key
CREATE DATABASE ENCRYPTION KEY
  WITH Algorithm = AES_128
  ENCRYPTION BY Server Certificate MyServer_Cert;
-- Enable the Database for Encryption by TDE
ALTER DATABASE AuthDB
  SET ENCRYPTION ON;
```

Encrypt Results DB:

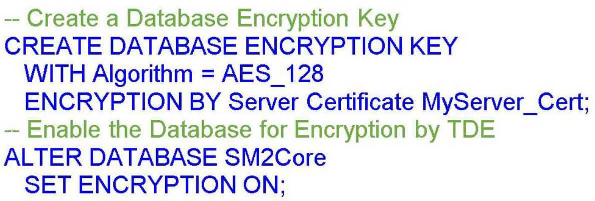
```
-- Move to the database you wish to enable TDE on
USE ResultsDB
GO
-- Create a Database Encryption Key
CREATE DATABASE ENCRYPTION KEY
  WITH Algorithm = AES_128
  ENCRYPTION BY Server Certificate MyServer_Cert;
-- Enable the Database for Encryption by TDE
ALTER DATABASE ResultsDB
  SET ENCRYPTION ON;
```

Encrypt Fin DB:

```
-- Move to the database you wish to enable TDE on
USE FinDB
GO
-- Create a Database Encryption Key
CREATE DATABASE ENCRYPTION KEY
  WITH Algorithm = AES_128
  ENCRYPTION BY Server Certificate MyServer_Cert;
-- Enable the Database for Encryption by TDE
ALTER DATABASE FinDB
  SET ENCRYPTION ON;
```

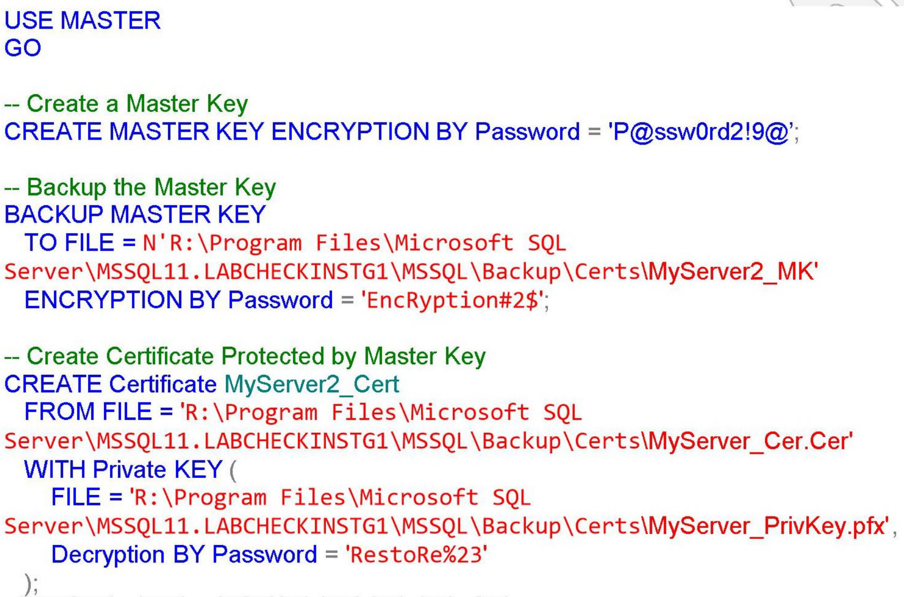
Encrypt SM2Core DB:

```
-- Move to the database you wish to enable TDE on
USE SM2Core
GO
```



```
-- Create a Database Encryption Key
CREATE DATABASE ENCRYPTION KEY
  WITH Algorithm = AES_128
  ENCRYPTION BY Server Certificate MyServer_Cert;
-- Enable the Database for Encryption by TDE
ALTER DATABASE SM2Core
  SET ENCRYPTION ON;
```

Encrypt Secondary SQL Server with Encryption Key and Primary DB Certificate:



```
USE MASTER
GO

-- Create a Master Key
CREATE MASTER KEY ENCRYPTION BY Password = 'P@ssw0rd2!9@';

-- Backup the Master Key
BACKUP MASTER KEY
  TO FILE = N'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\Certs\MyServer2_MK'
  ENCRYPTION BY Password = 'EncRyption#2$';

-- Create Certificate Protected by Master Key
CREATE Certificate MyServer2_Cert
  FROM FILE = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\Certs\MyServer_Cer.Cer'
  WITH Private KEY (
    FILE = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\Certs\MyServer_PrivKey.pfx',
    Decryption BY Password = 'RestoRe%23'
  );
```

Add Databases to Always ON in Primary Server:

Connect to Primary Replica Server: Add Database to Always ON

```
USE master
go
ALTER AVAILABILITY GROUP [LABCHECKINSTAGING] ADD DATABASE [elabsDB]

USE master
go
ALTER AVAILABILITY GROUP [LABCHECKINSTAGING] ADD DATABASE [ResultsDB]

USE master
go
ALTER AVAILABILITY GROUP [LABCHECKINSTAGING] ADD DATABASE [AuthDB]

USE master
go
ALTER AVAILABILITY GROUP [LABCHECKINSTAGING] ADD DATABASE [FinDB]

USE master
go
ALTER AVAILABILITY GROUP [LABCHECKINSTAGING] ADD DATABASE [SM2Core]
```

Connect to Primary Replica Server- Create a Full Backup

```
BACKUP DATABASE [elabsDB]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\elabsDB.bak'
WITH Copy_Only;
GO

BACKUP DATABASE [ResultsDB]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\ResultsDB.bak'
WITH Copy_Only;
GO

BACKUP DATABASE [AuthDB]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\AuthDB.bak'
WITH Copy_Only;
GO

BACKUP DATABASE [FinDB]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\FinDB.bak'
WITH Copy_Only;
GO

BACKUP DATABASE [SM2Core]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\SM2Core.bak'
WITH Copy_Only;
GO
```

Connect to Secondary Replica Server- Start the restoration process to bring your database to a synchronized state

```
RESTORE DATABASE [elabsDB]
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\elabsDB.bak'
WITH NoRecovery;
GO

RESTORE DATABASE [ResultsDB]
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\ResultsDB.bak'
WITH NoRecovery;
GO

RESTORE DATABASE [AuthDB]
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\AuthDB.bak'
WITH NoRecovery;
GO

RESTORE DATABASE [FinDB]
```

```
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\FinDB.bak'
WITH NoRecovery;
GO

RESTORE DATABASE [SM2Core]
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\SM2Core.bak'
WITH NoRecovery;
GO
```

Connect to Primary Replica Server- Create a TLog Backup

```
BACKUP LOG [elabsDB]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\elabsDB_TL.trn';
GO

BACKUP LOG [ResultsDB]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\ResultsDB_TL.trn';
GO

BACKUP LOG [AuthDB]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\AuthDB_TL.trn';
GO

BACKUP LOG [FinDB]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\FinDB_TL.trn';
GO

BACKUP LOG [SM2Core]
TO DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\SM2Core_TL.trn';
GO
```

Connect to Secondary Replica Server – Start the restoration process to bring your database to a synchronized state

```
RESTORE LOG [elabsDB]
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\elabsDB_TL.trn'
WITH NoRecovery;
GO

RESTORE LOG [ResultsDB]
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\ResultsDB_TL.trn'
WITH NoRecovery;
GO

RESTORE LOG [AuthDB]
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\AuthDB_TL.trn'
WITH NoRecovery;
```

```
GO

RESTORE LOG [FinDB]
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\FinDB_TL.trn'
WITH NoRecovery;
GO

RESTORE LOG [SM2Core]
FROM DISK = 'R:\Program Files\Microsoft SQL
Server\MSSQL11.LABCHECKINSTG1\MSSQL\Backup\SM2Core_TL.trn'
WITH NoRecovery;
GO
```

Connect to Secondary Replica Server- Join the Database to the AAG and bring it into the readable synchronized status

```
USE master
go
ALTER DATABASE elabsDB SET HADR AVAILABILITY GROUP = [LABCHECKINSTAGING];

USE master
go
ALTER DATABASE ResultsDB SET HADR AVAILABILITY GROUP = [LABCHECKINSTAGING];

USE master
go
ALTER DATABASE AuthDB SET HADR AVAILABILITY GROUP = [LABCHECKINSTAGING];

USE master
go
ALTER DATABASE FinDB SET HADR AVAILABILITY GROUP = [LABCHECKINSTAGING];

USE master
go
ALTER DATABASE SM2Core SET HADR AVAILABILITY GROUP = [LABCHECKINSTAGING];
```

Verify the status of Database Encryption:

```
USE master;
GO
SELECT db.name, db.is_encrypted, dm.encryption_state, dm.percent_complete,
dm.key_algorithm, dm.key_length
FROM sys.databases db LEFT OUTER JOIN sys.dm_database_encryption_keys dm ON
db.database_id = dm.database_id;
GO
```

SQL Server – Restoring a TDE Encrypted Database to a Different Server

HERE

Restoring a database to a different SQL Instance is usually a straightforward task. However, this attempt will return an error as shown below for an encrypted database when restoring into a different instance.

```
USE [master]
RESTORE DATABASE AuthDB FROM
DISK = N'G:\Program Files\Microsoft SQL Server\MSSQL11.SECRETNAME1\MSSQL\Backup\AuthDB.bak'
WITH FILE = 1, NOUNLOAD,  REPLACE,  STATS = 5
```

Output:

```
Msg 33111, Level 16, State 3, Line 2
Cannot find server certificate with thumbprint..
Msg 3013, Level 16, State 3, Line 2
RESTORE DATABASE is terminating abnormally
```

To restore successfully, we will need to physically copy the certificate (.cer) and private key (.pvk) to the destination server. As a best practice, we should immediately back up the certificate and the private key when we enable TDE. However, we can still take backup the certificate and private key now in the source server as shown below if not done earlier.

```
USE master;
GO
BACKUP CERTIFICATE TDECert1
TO FILE = 'E:\Backup\certificate_TDE_Test_Certificate.cer'
WITH PRIVATE KEY
(FILE = 'E:\Backup\certificate_TDE_Test_Key.pfx',
ENCRYPTION BY PASSWORD = 'Password12#')
```

Create a Master Key in destination server.

The password provided here is different from the one we used in the source server since we are creating a new master key for this server.

```
USE master
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'D1ffPa$$w0rd'
```

After a master key has been created, create a certificate by importing the certificate we created earlier. Here the 'Decryption By Password' parameter is same as that provided to export the certificate to a file.

```
CREATE CERTIFICATE TDECert2
FROM FILE = 'G:\Program Files\Microsoft SQL
Server\MSSQL11.SECRETNAME1\MSSQL\Backup\172.20.1.62_certs\MyServer_Cer.cer'
WITH PRIVATE KEY (FILE = 'G:\Program Files\Microsoft SQL
Server\MSSQL11.SECRETNAME1\MSSQL\Backup\172.20.1.62_certs\MyServer_PrivKey.pfx',
DECRYPTION BY PASSWORD = 'RestoRe%23')
```

Restore Database in destination server

We will now be able to restore the encrypted database backup successfully.

```
USE [master]
RESTORE DATABASE AUTHDB FROM DISK = N'G:\Program Files\Microsoft SQL
Server\MSSQL11.SECRETNAME1\MSSQL\Backup\AuthDB.bak'
WITH FILE = 1, NOUNLOAD, REPLACE, STATS = 5

USE [master]
RESTORE DATABASE FINDB FROM DISK = N'G:\Program Files\Microsoft SQL
Server\MSSQL11.SECRETNAME1\MSSQL\Backup\FinDB.bak'
WITH FILE = 1, NOUNLOAD, REPLACE, STATS = 5
```

EXHIBIT G

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 11/19/2020

ERIC CADDENHEAD (CADDENHEAD), previously interviewed, was interviewed at his residence located at [redacted] Milpitas, California. Also present for the interview was Assistant United States Attorney (AUSA) Vanessa Baehr-Jones. Prior to the interview, AUSA Baehr-Jones advised CADDENEHAD it was illegal to lie to a Federal Officer (Title 18 U.S.C. 1001) and CADDENHEAD confirmed he understood. After being advised of the identity of the interviewing parties CADDENHEAD agreed to the interview being audio recorded.

The below is an interview summary. It is not intended to be a verbatim account and does not memorialize all statements made during the interview. Communications by the parties were electronically recorded. The recording captures the actual words spoken. The interview was recorded and a copy of the recording will be maintained in the attached 1A and the 1D section of the case file.

While at Theranos CADDENHEAD's role was primarily focused on corporate structures. Additionally, CADDENHEAD worked on Theranos' launch with Walgreens. CADDENHEAD also supported ANTTI KORHONEN on the production side then the software guys would come in and do their thing. After CADDENHEAD was let go during a round of layoffs, KORHONEN fought to get him hired back. KORHONEN was promoted, but he got frustrated with everything because it was so chaotic so he left Theranos for another job, leaving CADDENHEAD as basically the last IT person at the company. After KORHONEN left there was another round of layoffs. During this time CADDENHEAD was responsible for collection employees computers when they left.

CADDENHEAD then took a job at ClimateWorks, and advised Theranos to hire an IT consulting group to help with the shutdown and said he would be willing to help by consulting. Then it was turned over to Sherwood, and CADDENHEAD had to execute a consulting agreement with Sherwood in order to

Investigation on 10/07/2020 at Milpitas, California, United States (In Person)

File # 318A-SF-7315857 Date drafted 10/07/2020

by Mario C. Scussel

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

help Neetek, the IT consulting company Theranos had hired to help with the shutdown of Theranos. CADDENHEAD worked remotely when he was consulting for Theranos. At this time he was still using his Theranos email address because it would allow him to VPN into the system. CADDENHEAD thought he might have had some emails which went to his personal email after Sherwood became involved.

Neetek_000815 to Neetek_000817

CADDENHEAD was shown Neetek_000815 to Neetek_000817, an email chain title "RE: LIS copies - need Eric or Antti" which started on July 24, 2018 and included XAN WHITE (WHITE), JOHN MCCHESNEY (MCCHESNEY) and MICHAEL CHUNG (CHUNG).

The software group made a copy of the production database and stored it on one of the servers and that was what they asked CADDENHEAD and CHUNG to copy. They then put the LIS database on three USB drives. MCCHESNEY had the three blank hard drives in his office and CHUNG was supposed to retrieve the drives and prep them onto the production server so they could copy the LIS database back-up copy onto the three hard drives. CADDENHEAD did assist with this task by VPNing into the production network and copying the binary for the LIS database onto the hard drives. CHUNG then took the hard drives with the copies and gave them back to MCCHESNEY. However, CADDENHEAD never had access to the information on the LIS database because this information was encrypted and he did not have the encryption key. CADDENHEAD thought there should also be an email from him in which he advises that the copies had been completed.

Neetek_000811 and Neetek_000746

CADDENHEAD was shown Neetek_000811 and Neetek_000746 an email titled "RE: Decrypted version" between CHUNG, CADDENHEAD, and MCCHESNEY starting on August 8, 2018 to August 10, 2018. CADDENHEAD advised that the private key was to decrypt the LIS database. In the emails they discuss a password list which had been given to KORHONEN. CADDENHEAD could copy the LIS database without the private key needed to access the data in the database.

Email from KORHONEN

CADDENHEAD was shown an email from KORHONEN from August 8, 2018 titled

"Decrypted Version in which CADDENHEAD forwarded the email "RE: Decrypted version" to KORHONEN, asking if he had this password document with the private key. CADDENHEAD had been asked to get in touch with KORHONEN. KORHONEN told CADDENHEAD that he had it at one time, but did not have it anymore. This document was an Excel document, which was encrypted through Microsoft RMS. CADDENHEAD ended up getting a copy of the Excel document, but could not get into it because he did not have the password to the document. CADDENHEAD was not as concerned with the database password because he could still make the copies of the binaries without this password. MCCHESNEY wanted the whole package which would include the copy and the password so they could decrypt the database. CADDENHEAD did not talk to MCCHESNEY or TAYLOR directly about the fact that they could not get into the database, but did talk to CHUNG about it. CADDENHEAD advised that without the private encryption key one would not be able to get into the documents.

SIVA DEVABAKTHINI (DEVABAKTHINI), who was referred to in one of the emails was the person who had advised that the encryption key would have been in the encrypted excel document which he had provided to KORHONEN. DEVABAKTHINI left Theranos in September 2016 according to the email.

Neetek_000576 - Neetek_000577

CADDENHEAD was shown Neetek_000576 - Neetek_000577 an email chain which started on June 6, 2018 an included an email from SEKHAR VARIAM (VARIAM) titled "RE: LIS data base discussion - response to request". CADDENHEAD never spoke with VARIAM about the LIS database. CADDENHEAD only cared about where the LIS database was so that he could copy the files onto the hard drives. One could only decrypt the database with the master key, but once RMS was shutdown they would not be able to decrypt the database.

The end of the email chain was an email from TAYLOR on September 2, 2018 forwarding an email from VARIAM on August 30, 2018 in which VARIAM forwarded his email from June 6, 2018. CADDENHEAD was not surprised TAYLOR was asking for information as to how to put the LIS database back together, because TAYLOR was not a "tech guy" so he did not understand.

CADDENHEAD did not recall receiving these emails from September as they went to his Theranos email and he was done with the Theranos project by this time. Accordingly he had stopped checking his Theranos email.

Neetek_000616

CADDENHEAD was shown Neetek_000616 an email from SHEKAR CHANDRASEKARAN (CHANDRASEKARAN) which TAYLOR forwarded on August 28, 2018 titled "Call re LIS (priv/conf) - time sensitive". CADDENHEAD advised that CHANDRASEKARAN was the main person for software. CHANDRASEKARAN would have had administrative rights to the whole LIS system. CADDENHEAD had no idea why CHANDRASEKARAN was providing his credentials and password to TAYLOR. CADDENHEAD also did not know why they wanted to make another copy of the LIS database.

CADDENHEAD advised that CHANDRASEKARAN's group who were responsible for the software portion of the LIS database and should have had all the encryption keys for the database. CADDENHEAD did not know why CHANDRASEKARAN did not respond to these emails to provide that decryption information. CHANDRASEKARAN's software development group was under their own control and did their own thing. This group had reported up to SUNNY BALWANI (BALWANI) who was friends with CHANDRASEKARAN.

Neetek_000591

CADDENHEAD was shown Neetek_000591, an email titled "LIS" on August 29, 2018 between CHUNG, CADDENHEAD, TAYLOR, CHANDRASEKARAN, and MCCHESNEY.

On Friday August 31, 2018 the Newark facility was shut down, and it would have been very difficult to get the LIS working again because every single hard drive in the disk array was encrypted independently of each other, so if you got them out of order then the system would not work.

CADDENHEAD was not aware of an effort to put the information from the LIS onto Excel spreadsheets. CADDENHEAD thought the LIS database was too large and could not be put on Excel spreadsheets. If the database was up and running then they might be able to run a report for each patient in the database, but CADDENHEAD never used the LIS database himself so he was not certain.

Neetek_000578

CADDENHEAD was shown Neetek_000591, an email titled "RE: Info for Shekar" between TAYLOR, CADDENHEAD and CHUNG on September 2, 2018. This email would have been after Newark was shutdown. CADDENHEAD was not sure why TAYLOR was requesting the information in this email.

CADDENHEAD advised that TAYLOR was asking the wrong people these questions as he should have instead been asking CHANDRASEKARAN and the software team. The only thing CADDENHEAD was able to do on the list in this email was to make a copy of the binary.

<u>Neetek_000333 - Neetek_000338</u>

CADDENHEAD was shown Neetek_000333 through Neetek_000338, an email chain from August 28, 2018 to September 19, 2018 with the subject "RE: Call re LIS (priv/conf) - time sensitive" which included CADDENHEAD, MORAN, JAROD WADA (WADA), TARYN MCCARTHY, and CAMILLE JOHNSON. In this email chain MORAN was asking CADDENHEAD to make a copy of the LIS software from the share drive, which was the code for the LIS. CADDENHEAD did not talk to her about this and did not think MORAN got a copy of the LIS database, as only MCCHESNEY had the copies of the LIS database. CADDENHEAD advised that MORAN's request for the code for the LIS to be copied onto a hard drive never happened.

CADDENHEAD did not recall having a conversation with MORAN about this request and advised that MORAN rarely picked up her phone when he called.

MORAN had also been involved at Theranos prior to 2018 when IT was copying emails.

CADDENHEAD did not know what she meant by "we are working on a solution". CADDENHEAD thought that the 40 GB he referred to in his email on September 4, 2018 was the size of the LIS database. He would have been able to get the information about the size of the database from the back-ups he had created previously.

CADDENHEAD was not replying to the emails as he did not have a contract with Wilmer Hale, instead his contract was with Sherwood, so he was not sure if he was cleared to speak with her directly by Sherwood, as everything had to be cleared with Sherwood.

CADDENHEAD never spoke with MORAN about the private key/encryption password for the LIS database and not being able to obtain this password.

CADDENHEAD did not know where the copies he made of the LIS database went after CHUNG provided them to MCCHESNEY. The only person CADDENHEAD was communicating with at this time was CHUNG.

CADDENHEAD thought it had to have been expressed that the software group would be be the ones who had the encryption passwords during these conversations.

CHANDRASEKARAN was good friends with BALWANI from working together at a previous software company, possibly Microsoft. CADDENHEAD thought either CHANDRASEKARAN might have told him about the fact that he had worked with BALWANI previously, or he learned it from KORHONEN.

BALWANI used his own encryption and bypassed using RMS. IN particular, BALWANI would encrypt excel documents for anything related to financial numbers. This included any documents BALWANI sent to Theranos' controller DANISE YAM (YAM). CADDENHEAD knew this from when he worked previously with MORAN on collecting emails and documents. CADDENHEAD would flag documents for MORAN which he could not open, by sending her an email. CADDENHEAD recalled the BALWANI was still at Theranos at the time, because they were still working out of Theranos' Palo Alto facility. BALWANI had provided some of his passwords, which worked on some of the documents, but it the document had to do with financials the password did not work. Accordingly, none of the financials sent to YAM could be accessed with the passwords provided by BALWANI. CADDENHEAD did not recall any financials which had been sent outside of Theranos.

EXHIBIT H

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/07/2020

MICHAEL CHUNG (CHUNG), business telephone number [redacted], email address [redacted], was interviewed via telephone. Also present for the interview were Assistant United States Attorney (AUSA) John Bostic and AUSA Vanessa Baehr-Jones. Prior to the interview, AUSA Bostic advised CHUNG it was illegal to lie to a Federal Officer (Title 18 U.S.C. 1001) and CHUNG confirmed he understood. After being advised of the identity of the interviewing parties and the nature of the interview, CHUNG provided the following information:

CHUNG works for a company called Neetek, which was first contacted by someone from Theranos because they wanted to have their servers moved because they were discontinuing their lease. Accordingly they needed to vacate the building and wanted to move their servers to a datacenter. Theranos then called Neetek again because they were ending another lease and wanted to move their information to the cloud. Finally, attorneys from Irell Manella contacted Neetek because they wanted access to the cloud data. These attorneys represented Fortress Investment Group, which at that point owned part of Theranos. The information on the cloud which these attorneys from Irell Manella were looking for were files which were not related to the Laboratory Information System Database (LIS).

The first work CHUNG did for Theranos was to move servers. In July 2018 CHUNG met with JOHN MCCHESNEY (MCCHESNEY), who had contacted Neetek, in regards to moving servers from Newark to a datacenter as Theranos was trying to get out of their Newark facility. When MCCHESNEY first called Neetek he did not understand the complexity of moving the infrastructure, but Neetek informed him as to what the process would require. Neetek's first step was to figure out what Theranos had at the Newark facility which needed to be moved. There were a number of custom applications, like LIS, on the servers located in Newark, California. They decided not to move the LIS at this time, and instead they decided to have people pull all of the information

Investigation on 04/23/2020 at San Francisco, California, United States (Phone)

File # 318A-SF-7315857 Date drafted 04/23/2020

by Mario C. Scussel

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

from the LIS. CHUNG thought this decision might have been made because they could not move data when Theranos had and in-house software team which was not there any longer. Accordingly the decision was made to only move the Corporate infrastructure at this time. Approximately three to four Theranos employees then began running reports out of LIS to save this data. While CHUNG did not know the names of those from Theranos who were pulling these reports, he thought MCCHESNEY might know their names.

When Theranos employees were backing up the LIS by running reports, they were saving information on spreadsheets which were to be saved on the corporate infrastructure so the information was not lost. While CHUNG never saw these reports saved on the corporate infrastructure, there was no where else they could have gone. These spreadsheets could not be queried for information as they would have been in the database.

When MCCHESNEY was trying to wind things down and dissolve Theranos, they needed to move information to the datacenter and still be able to access the corporate data needed in order to dissolve the company. The datacenter where they moved the servers was Centurylink in Sunnyvale, California.

Neetek figured out what in the server room was related to corporate data and moved that to Centurylink. Everything else went to a public storage facility. On the day they shut everything down at Newark, CHUNG, MCCHESNEY, and the facilities guy at Theranos transported the corporate data to Centurylink and then the rest to public storage. They placed everything on the same truck and dropped the corporate data off at Centurylink first. CHUNG and his team were waiting for MCCHESNEY to drop off the equipment at Centurylink.

MCCHESNEY was the main person at Theranos who CHUNG worked with and reported to. He also worked with a PHILLIPE Last Name Unknown (LNU) who CHUNG understood to be the interim Chief Financial Officer at Theranos.

CHUNG thought the LIS would run without the corporate infrastructure as he did not think there were a lot of dependencies between the corporate infrastructure and the production infrastructure like LIS.

The production infrastructure stayed in storage for about a year or so, then JARED LNU (JARED) from Sherwood called because the equipment Lessor wanted their equipment back. JARED wanted help figuring out what was in storage and what they still had. CHUNG's team went to storage and confirmed the equipment was there, but found that all the hard drives had been removed. CHUNG's team then returned the equipment to the Lessor's vendor without the hard drives. CHUNG then recalled MCCHESNEY had asked him and his team to remove all the hard drives before they were placed on the truck. The hard drives were packed in separate boxes and taken to a different storage facility, but CHUNG did not know where they were taken. Prior to removing the hard drives, CHUNG reminded MCCHESNEY that they would not be able to get anything off these hard drives and MCCHESNEY confirmed he understood this. CHUNG got the impression MCCHESNEY did not want to be the person responsible for losing these drives or destroying the data even though there was no way of recovering the data from these hard drives.

CHUNG had meetings with MCCHESNEY and others at Theranos to explain that once the servers were turned off, then a forensic team would be needed to recover the data on the LIS, but nobody on their team knew how to do this or if it would even be possible. DAVID TAYLOR, interim Theranos CEO, would be present for some of these meetings with Neetek. It took two months with lots of meetings with Theranos to plan the move then three days to execute the move. Neetek estimated there was an 80% chance of getting the corporate email back up and running after they moved the servers to the datacenter. The corporate emails and files were what was most important to MCCHESNEY and Theranos. In regards to the production infrastructure, Neetek estimated that there was approximately a 0% chance of getting the information back. There was no way CHUNG's team could move the LIS and retain the information as they would have needed to reengage former Theranos IT employees and the contract software engineers.

MCCHESSNEY told CHUNG he had tried to get the software group to come back to help move the LIS database, but they declined.

Moving hundreds of devices with thousands of connections would be nearly impossible, which is why the percent chance of getting everything back up and running was so low. They discussed trying to move the LIS without taking it apart, but that was not possible. Additionally, a lot of the connectivity was virtual, located in the software. MCCHESNEY understood that the LIS would be lost once they moved it. This was the reason Theranos ran the reports which were to be saved on the Corporate infrastructure. Someone from Theranos confirmed that all the data from the LIS had been backed up. CHUNG recalled that right before they shut down the LIS to move it, someone from Theranos told them to wait because they had to pull one more report from LIS. Someone had made an announcement that the LIS was being shutdown and they wanted to wait until everyone was ready to shut it down.

There was also an LIS database copy which was done by ERIC CADDENHEAD (CADDENHEAD), a former Theranos IT employee who came in to make a copy of the LIS on to USB drives. In order to get the backup copy of the data base running, one would need to get the whole system running. There was a forensic way of extracting the data from the backup copy, but CHUNG's team did not know how to do this.

CHUNG thought the Theranos email system should still be alive, and JARED would be able to access it.

CHUNG also agreed to search his email for any emails or documents related to Theranos. On April 24, 2020 CHUNG provided a Microsoft Outlook data file containing all of the Theranos email he had retained which included the contract between Neeek and Theranos. CHUNG sent this in a zip file via email. CHUNG's email with the zip file, and an unzipped copy will be maintained in the attached 1A.

EXHIBIT I

RE: Summary of our conversation [privileged / confidential]

From: Eric Caddenhead <"/o=theranos organization/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=eric caddenhead824">
To: Xan White <xanwhite@theranos.com>
Date: Fri, 22 Jun 2018 21:36:23 +0000

My contact information:

Eric Caddenhead
[redacted]

From: Xan White
Sent: Friday, June 22, 2018 1:18 PM
To: Eric Caddenhead <ECaddenhead@theranos.com>
Subject: Summary of our conversation [privileged / confidential]

Eric,

Just to summarize our conversation this morning, regarding preservation matters.

Our servers are set to automatically back themselves up on a rolling basis, such that we have an incremental image of the data on the server every 24 hours (if not more frequently). That process will continue indefinitely, unless it is formally stopped. As long as the physical servers stay intact, the data on them is preserved, and can be accessed by someone with the proper password. At least Antti, John M., and you currently have that password.

Our backup tapes are at Iron Mountain. Ian McDowell and Antti have access to that.

You and I also covered a few items related to day-to-day IT matters. Our servers are set up consistent with ordinary industry practices, such that a skilled senior systems administrator should have no difficulty working within our systems.

Thanks for your willingness to work on a consulting basis; I'll get an agreement to you next week.

As you know, my main and pressing concern is data preservation, and our systems are set up to automatically preserve data on an ongoing basis, provided there is not a significant failure or physical destruction of the servers.

All best,

Xan White
Corporate Counsel
Office: 650.546.2218

Cell: 650.305.8391
7373 Gateway Blvd.
Newark, CA 94560

theranos

EXHIBIT J

From: Heller, Roger N.
Sent: Friday, September 14, 2018 1:00 PM EDT
To: oneill.stephen@dorsey.com
CC: Sobol, Michael W.; Gardner, Melissa; David Copley; 'Tanya Korkhov'; Moran, Katie; Casamassima, Chris
Subject: FW: In re Theranos: Request for Confirmation re Preservation of Evidence
Attachments: Heller Letter 9.6.18.pdf

Steve-

See the below (and attaching my September 6 letter for reference). Please confirm that Sherwood Partners will preserve all of Theranos' databases through the duration of the litigation.

Thanks,

-Roger

From: Moran, Katie [mailto:Katie.Moran@wilmerhale.com]
Sent: Friday, September 14, 2018 9:50 AM
To: Heller, Roger N.
Cc: Sobol, Michael W.; Gardner, Melissa; 'David Copley'; Tanya Korkhov; Casamassima, Chris; Romeo, Mike; kgoodhart@cooley.com; jlombard@cooley.com; steverummage@dwt.com; benbyer@dwt.com
Subject: RE: In re Theranos: Request for Confirmation re Preservation of Evidence

Roger:

We write in response to your September 6, 2018 letter requesting that Theranos confirm that it has taken appropriate measures to preserve potentially relevant ESI. Theranos has preserved its various databases, including the LIS database, on hard drives and plans to store those hard drives at Iron Mountain. As discussed on yesterday's call, all of Theranos' assets, including control of Theranos' databases, have been assigned to Sherwood Partners.

Katie

From: Heller, Roger N. <rheller@lchb.com>
Sent: Thursday, September 6, 2018 10:51 PM
To: Casamassima, Chris <Chris.Casamassima@Wilmerhale.com>; Moran, Katie <Katie.Moran@wilmerhale.com>; Romeo, Mike <Mike.Romeo@wilmerhale.com>; kgoodhart@cooley.com; jlombard@cooley.com; steverummage@dwt.com; benbyer@dwt.com
Cc: Sobol, Michael W. <MSOBOL@lchb.com>; Gardner, Melissa <mgardner@lchb.com>; 'David Copley' <dcopley@KellerRohrback.com>; Tanya Korkhov <tkorkhov@KellerRohrback.com>
Subject: In re Theranos: Request for Confirmation re Preservation of Evidence

Counsel, please see the attached letter.

Thanks,

-Roger

EXHIBIT K

To: Sunny Balwani[/O=THERANOS ORGANIZATION/OU=First administrative group/cn=recipients/cn=sbalwani]
From: Ian McDowell[/O=THERANOS ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=IMCDOWELL]
Sent: Wed 6/10/2015 5:12:18 PM (UTC)
Subject: Visio's of CoLo
Colo_ConnectionMap.vsdx
Colo_Rack.vsdx

Sunny,

Here are Visio's of the rack config and connectivity map.

-ian

From: Ian McDowell
Sent: Wednesday, June 10, 2015 9:47 AM
To: Sunny Balwani
Subject: CoLo BoM

Sunny,

We have finalized the BoM for our initial colo needs. Please see attached.

Breakdown (everything is in HA pairs, etc):

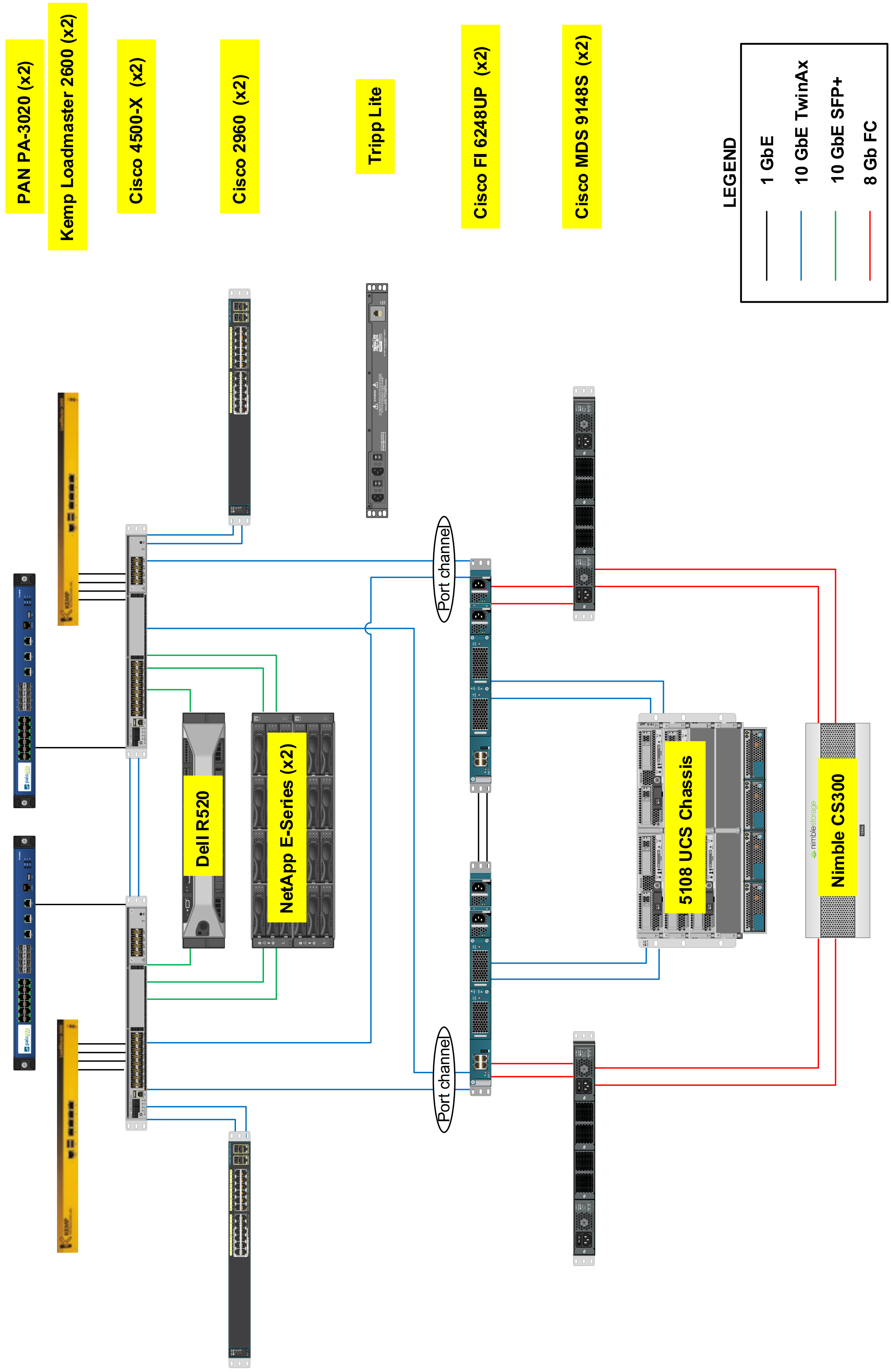
Palo Alto Networks firewalls
Kemp load balancers
Switches: 4500x (core), MDS (fiber Channel), and 2960's (access)
Tripplite console
Cisco UCS compute chassis with 4 2xsocket 256GB RAM blades (Vmware) and 2 2xsocket 128 GB RAM blades (SQL cluster)
Nimble Storage (fiber channel, 48TB controller and 60TB expansion shelf + cache acceleration)
VMware licenses with site recovery
Archive grade storage for backup
Backup media server
Commvault backup licenses

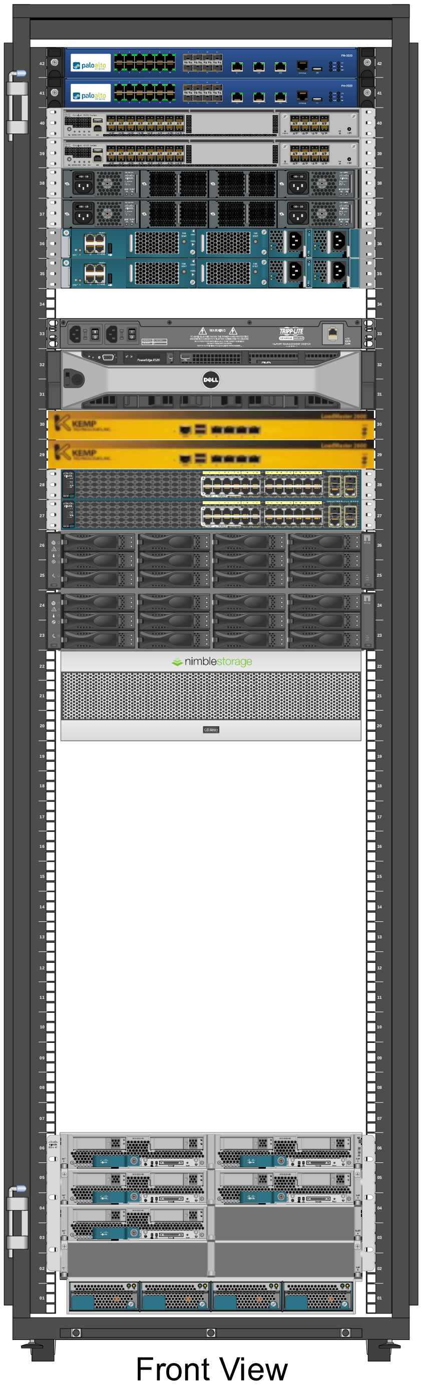
This was negotiated down from $800K to $476K with very aggressive discounts.

Please let me know if you want to schedule some time to go over everything by line item. I can get Danise involved to work on financing.

Thank you,
-ian

Ian McDowell
Senior IT Manager
Theranos, Inc.
(650) 470-6183
PRIVILEGED AND CONFIDENTIAL COMMUNICATION
IMPORTANT – This electronic transmission, and any files transmitted with it are confidential and/or legally privileged information. This information is intended solely for the use of the individual or entity to which it is addressed. Any disclosure, retransmission, reproduction, dissemination or other use of the contents of this information by persons or entities other than the intended recipient is strictly prohibited. If you have received this email in error, please contact us immediately and delete all copies. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of Theranos, Inc. Finally, before opening or using attachments the recipient should check this email and any attachments for the presence of viruses. Theranos, Inc. accepts no liability for any damage caused by any virus transmitted by this email. Our sole responsibility is limited to resupplying any affected attachments.
Theranos, Inc., 1701 Page Mill Road, Palo Alto, CA, 94304
650-838-9292 www.theranos.com


PAN PA-3020 (x2)
Kemp Loadmaster 2600 (x2)
Cisco 4500-X (x2)
Cisco 2960 (x2)
Tripp Lite
Cisco FI 6248UP (x2)
Cisco MDS 9148S (x2)
LEGEND
1 GbE
10 GbE TwinAx
10 GbE SFP+
8 Gb FC
Port channel
Port channel
Dell R520
NetApp E-Series (x2)
5108 UCS Chassis
Nimble CS300



PAN PA-3020 (x2)

Cisco 4500-X (x2)

Cisco MDS 9148S (x2)

Cisco FI 6248UP (x2)

Tripp Lite Console Switch

Dell PowerEdge R520

Kemp Loadmaster 2600 (x2)

Cisco 2960 (x2)

NetApp E-Series (x2)

Nimble CS300

5108 UCS Chassis

B200M4 blade servers (x8)

Front View

EXHIBIT L

ORIGINAL

DELL | Financial Services

Assigned to CIT Financial USA Inc.

THERANOS, INC.
MASTER LEASE AGREEMENT SCHEDULE NO. 001-6664412-500

THIS SCHEDULE IS SUBJECT TO AND INCORPORATES THE TERMS AND CONDITIONS OF MASTER LEASE AGREEMENT NO. 6664412 ("Agreement") DATED March 12, 2013 BETWEEN DELL FINANCIAL SERVICES L.L.C. ("Lessor") AND THERANOS, INC. ("Lessee"). If the entity named on this Schedule is not the Lessee named under the Agreement, then such entity, if an affiliate of Lessee approved in writing in advance by Lessor, shall be deemed the Lessee under this Schedule.

Lessor hereby agrees to lease and/or make available to Lessee subject to the terms, conditions and provisions set forth in this Schedule and in the Agreement, the Products described below. Any capitalized term used herein and not defined herein shall have the meaning ascribed to it in the Agreement.

PRODUCT DESCRIPTION AND LOCATION: See below or Exhibit "A" attached to and made a part hereof.

PRODUCT SELLER: INTERVISION, 2250 WALSH AVENUE, SANTA CLARA, CA 95050-2614

Product Description	Product Location	Lessee Purchase Order No.	Rent*	Primary Term (Mos.)	Commencement Date**
See Exhibit 'A'	See Exhibit 'A'	See Exhibit 'A'	**$6,219.61**	**48**	**May 1, 2013**

Total Product Acquisition Cost: $84,379.45

Rent is payable: **in arrears**

Payment Period: **Quarterly**

Pro-rated Rent: **applies** **$1,036.61**

* Lessee is responsible for applicable taxes, shipping and other amounts as described in the Agreement, and, with the first payment of Rent, any prorated Rent if applicable. Such amounts are further described in Exhibit "A".

** The Commencement Date may be extended for one Payment Period until the Schedule is returned in accordance with the terms stated in the Agreement. Lessor may charge Lessee prorated Rent accruing from the Acceptance Date to the Commencement Date, as such date is finally determined.

END OF LEASE OPTIONS: Provided that no Event of Default has occurred and is continuing at the expiration of the Lease Term, Lessee shall have the option to (i) purchase the Products for $1.00; or (ii) return the Products in accordance with the MLA for a disposal fee agreed upon by both parties.

SECURITY INTEREST: As a continuing security interest for Lessee's obligation hereunder, Lessee hereby grants to Lessor a first priority security interest in all of Lessee's rights and interests in and to the Products and all proceeds thereof, free and clear of all security interests, liens or encumbrances whatsoever.

MASTER LEASE AGREEMENT SCHEDULE NO. 001-6664412-500

COMPLETION OF SCHEDULE: Lessee hereby authorizes Lessor to insert or update the serial numbers of the Products from time to time as necessary.

If Lessee delivers this signed Schedule, any amendment or other document related to this Schedule or the Master Lease (each a "Document") to Lessor by facsimile transmission, and Lessor does not receive all of the pages of that Document, Lessee agrees that, except for any pages which require a signature, Lessor may supply the missing pages to the Document from Lessor's database which conforms to the version number at the bottom of the page. If Lessee delivers a signed Document to Lessor as an e-mail attachment, facsimile transmission or by U.S. mail, Lessee acknowledges that Lessor is relying on Lessee's representation that the Document has not been altered. Lessee further agrees that, notwithstanding any rule of evidence to the contrary, in any hearing, trial or proceeding of any kind with respect to a Document, Lessor may produce a tangible copy of the Document transmitted by Lessee to Lessor by facsimile or as an e-mail attachment and such signed copy shall be deemed to be the original of the Document. To the extent (if any) that the Document constitutes chattel paper under the Uniform Commercial Code, the authoritative copy of the Document shall be the copy designated by Lessor or its assignee, from time to time, as the copy available for access and review by Lessee, Lessor or its assignee. All other copies are deemed identified as copies of the authoritative copy. In the event of inadvertent destruction of the authoritative copy, or corruption of the authoritative copy for any reason or as the result of any cause, the authoritative copy may be restored from a backup or archive copy, and the restored copy shall become the authoritative copy. At Lessor's option, this electronic record may be converted into paper form. At such time, such paper copy will be designated or marked as the authoritative copy of the Document.

By signing below, each of the parties hereto agrees to be bound by the terms of the Agreement, this Schedule and the attached Exhibit "A".

THERANOS, INC.
(Lessee)

By: ______________________
(Authorized Signature)

[illegible] IT Manager
(Name/Title)

5/8/2013
(Date)

DELL FINANCIAL SERVICES L.L.C.
(Lessor)

By: ______________________
(Authorized Signature)

5/13/13
(Name/Title)

Gregory DeKock
(Date) Director Operations

THERANOS, INC.

LEASE SCHEDULE

No.006664412-500

EXHIBIT A

5/1/2013

4/30/2017

Qty	Item #	Service Tag	Item Description	Periodic Rent	Lease Start	Lease End	Equipment Location	LRF Asset	Asset Type	Total Equiptment Cost	Upfront Tax
1	DELLONLDEC11199	GN8MDV1	DELL UPS RACK 5600W 4U HEONLINE 208				7333 GATEWAY BLVD	0.07371	H		
			001432.0000 INV# 52416	**$245.10**	**5/1/2013**	**4/30/2017**	**7333 GATEWAY BLVD**	**0.07371**	**H**	**$3,050.67**	**$274.55**
1	DELLONLDEC11198	HBSNZX1	DELL POWERCONNECT M6348.48 GBE PORTS MA				7333 GATEWAY BLVD	0.07371	H		
1	DELLONLDEC11198	2CSNZX1	DELL POWERCONNECT M6348.48 GBE PORTS MA				7333 GATEWAY BLVD	0.07371	H		
1	DELLONLDEC11198	JBSNZX1	DELL POWERCONNECT M6348.48 GBE PORTS MA				7333 GATEWAY BLVD	0.07371	H		
1	DELLONLDEC11198	1CSNZX1	DELL POWERCONNECT M6348.48 GBE PORTS MA				7333 GATEWAY BLVD	0.07371	H		
			001432.0000 INV# 52416	**$845.40**	**5/1/2013**	**4/30/2017**	**7333 GATEWAY BLVD**	**0.07371**	**H**	**$10,522.28**	**$947.00**
1	DELLONLDEC11198	GBSNZX1	DELL EQUALOGIC PS - M4110XS 10GB STOREA				7333 GATEWAY BLVD	0.07371	H		
			001432.0000 INV# 52416	**$1,920.45**	**5/1/2013**	**4/30/2017**	**7333 GATEWAY BLVD**	**0.07371**	**H**	**$23,902.89**	**$2,151.28**
1	DELLONLDEC11198	CBSNZX1	DELL POWEREDGE M620 BLADE SERVE R				7333 GATEWAY BLVD	0.07371	H		
1	DELLONLDEC11198	FBSNZX1	DELL POWEREDGE M620 BLADE SERVE R				7333 GATEWAY BLVD	0.07371	H		
1	DELLONLDEC11198	BBSNZX1	DELL POWEREDGE M620 BLADE SERVE R				7333 GATEWAY BLVD	0.07371	H		
1	DELLONLDEC11198	DBSNZX1	DELL POWEREDGE M620 BLADE SERVE R				7333 GATEWAY BLVD	0.07371	H		
			001432.0000 INV# 52416	**$2,262.07**	**5/1/2013**	**4/30/2017**	**7333 GATEWAY BLVD**	**0.07371**	**H**	**$28,154.84**	**$2,533.93**
1	DELLONLDEC11198	9BSNZX1	DELL BLADE SERVER ENCLOSURE NO BLADESM				7333 GATEWAY BLVD	0.07371	H		
			001432.0000 INV# 52416	**$946.59**	**5/1/2013**	**4/30/2017**	**7333 GATEWAY BLVD**	**0.07371**	**H**	**$11,781.66**	**$1,060.35**
			Totals:	**$6,219.61**						**$77,412.34**	**$6,967.11**
			(excluding applicable taxes)								

EXHIBIT M

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 12/16/2020

MICHAEL CHUNG (CHUNG), previously interviewed, was interviewed via WebEx video teleconference. Representing CHUNG during the interview were Ed Swanson and Carly Bittman from Swanson & McNamamra. Also present from the government were Assistant United States Attorney (AUSA) Vanessa Baehr-Jones and AUSA Bob Leach. This interview was conducted pursuant to a Proffer Agreement signed by CHUNG, Swanson, and AUSA Baehr-Jones. Prior to the interview Swanson reviewed the Proffer Agreement with CHUNG as did AUSA Leach. AUSA Leach reviewed the importance of being truthful and that lying would be a violation of 18 USC 1001. After being advised of the identity of the interviewing parties and the nature of the interview, CHUNG provided the following information:

CHUNG was the sole owner of Neetek, an IT Services company which had approximately ten employees. Neetek specialized in project delivery and would help companies and their IT departments with things they did not have time to do themselves, such as moves.

Neetek was first introduced to Theranos by Coyote Creek Consulting which called Neetek and offered them the Theranos job because the work Theranos wanted done was not a fit for their company. At first, the Theranos project sounded like it was an office move, which was Neetek's specialty. After advising Coyote Creek Consulting that Neetek was willing to take the job, CHUNG then got a call from JOHN MCCHESNEY (MCCHESNEY) who hired Neetek to move Theranos' servers.

The Theranos project changed from a move from a big office to a small office to a move to a data center. While this meant Neetek did not have to worry about setting up desks and VPN's, there were other concerns they would have to deal with in the move to the data center.

CHUNG learned about the LIS database when MCCHESNEY asked him to move

Investigation on 12/07/2020 at San Francisco, California, United States (Phone, Other (Videoteleconference))

File # 318A-SF-7315857 Date drafted 12/08/2020

by Mario C. Scussel

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

it. However, CHUNG advised MCCHESNEY that they could not move the LIS database. While CHUNG and Neetek had experience moving Microsoft systems, the LIS database was a bespoke database developed by a group of software engineers who no longer worked at Theranos and they would be needed in order to help move the database. CHUNG advised MCCHESNEY that they would not be able to move the database and they would need the software engineers to move it. There were meetings where CHUNG had to advise that they could not move the database and the reasons they could not move it. MCCHESNEY was not only present for these meetings, but he also commented during the meetings that that the LIS database could not be moved. DAVID TAYLOR (TAYLOR) was also present for these calls/meetings as was XAN WHITE (WHITE) and people from Wilmer Hale.

CHUNG was shown Neetek_000855 which contained an email from WHITE to MCCHESNEY and TAYLOR on July 18, 2018 which advised "It also appears to require passwords that Antti (Korhonen) alone may have, though that's not clear to me." CHUNG had tried to reach ANTTI KORHONEN (KORHONEN) multiple times to get the password, but never got in touch with him. ERIC CADDENHEAD (CADDENHEAD) also reached out to KORHONEN to try to get the password for the LIS database because they were friends. However, neither CHUNG nor CADDENHEAD was ever able to get a hold of KORHONEN, and CHUNG has never spoken with KORHONEN at any point. CHUNG had advised MCCHESNEY that CADDENHEAD could not get a hold of KORHONEN in order to obtain the password.

The LIS database was up and running on August 18, 2018 and continued until the date which Neetek took everything down.

Someone had purchased three USB drives to copy the data from the LIS database onto each drive. CADDENEHAD accessed the system remotely and initiated the copies. At this point CHUNG was just doing what MCCHESNEY asked him to do. CHUNG had told MCCHESNEY that these USB drives would need a password, which they did not have, in order to access the data on the drives. As a result, copying the data to these hard drives would not be useful because the LIS ran on complex software which they did not have any support for and it had hundreds of pieces of equipment. Additionally, one would need the binaries, source code, and other items to make the database function again. CHUNG told MCCHESNEY that they would need other things to reconstruct the LIS database, but he might not have been so specific as to name the things they would need, such as the Binaries.

After the USB drives were copied, CHUNG gave the three copies to MCCHESNEY who said he was going to send them to law firms. CHUNG did not know why they made three copies of the LIS database, at the time he just thought that they had made extra back-ups.

CHUNG was shown Neetek_000746 an email from CHUNG to MCCHESNEY on August 10, 2018 titled "Decrypted Version". Part of the email stated "The password for restoring the private key should be in a document that Antti had in his possession (Siva Devabakthini sdevabakthini@theranos.com, the Dev-ops engineer provided Antti with a document containing all the passwords before he left in 2016 September)." CHUNG never reached out to SIVA DEVABAKTHUNI (DEVABAKTHUNI). CHUNG sent this email because they were trying to figure out how to reconstruct the the data and the instructions said they needed a password.

CHUNG did email with SHEKAR CHANDRASEKARAN (CHANDRASEKARAN), who was the only person he had contacted in the software group. It was possible CHUNG was on some calls with CHANDRASEKARAN, but he was not sure. CHUUNG did not recall any emails from CHANDRASEKARAN about the password. However CHUNG did recall emails from CHANDRASEKARAN asking for assistance.

The day they were moving everything out of Theranos, CHUNG asked if they were ready to shut everything down and he was told to wait for a bit because someone was running spreadsheets/reports from the LIS database. Then when this person was done MCCHESNEY said they could shut it down.

MCCHESNEY was frustrated by the news that the LIS would not be able to be revived, as nobody wants to hear that it would be extremely hard or impossible to recreate something. MCCHESNEY did not mention to CHUNG that the government had subpoenaed the LIS database. CHUNG did not know who subpoenaed the LIS database, as he was just doing what MCCHESNEY and CADDENHEAD told him to do.

CHUNG was shown Neetek_000599 to Neetek_000600 an email from TAYLOR to KATIE MORAN (MORAN), CHANDRASEKARAN, CHUNG, and CADDENHEAD on August 28, 2018 titled "Call re LIS (priv/conf) - time sensitive". CHUNG recalled this meeting being similar to a meeting which happened much before this one. TAYLOR's statement in the email that the LIS database would be "very difficult to resuscitate" was consistent with CHUNG's message to MCCHESNEY. CHUNG did not recall a conversation during this call about why it would be difficult to resuscitate the database, but thought that everyone should have already known the reasons by this time. Either during or after this call CHANDRASEKARAN sent a list of the things he needed to resuscitate the database. CHUNG did not recall having any conversations with MORAN prior to this meeting, and he never met her in person. While MORAN spoke during this meeting, CHUNG could not recall what she said. The need for a password was discussed many times, but CHUNG could not recall if it was discussed again during this specific meeting. CHUNG was consistent in his message to Theranos that the password from KORHONEN was necessary to access the LIS database data.

In the August 29, 2018 email CHUNG was working to obtain the binaries because these would be needed to reconstruct the LIS database. However, this would not be enough to resuscitate the database because this was just part of the list of things they would need to complete the reconstruction.

On September 2, 2018 TAYLOR sent an email to CADDENHEAD asking for four items for CHANDRESEKARAN. When CHUNG was asked to copy the binaries he had already had the conversation on multiple occasions that this would not solve the problem. At this point, CHUNG was just trying to do what he was asked to do. The LIS database had already been taken down by this point.

CHUNG was not surprised TAYLOR was asking to resuscitate the LIS database just days after he said it would be very difficult to resuscitate because this type of thing happened to CHUNG often where a client would ask for something even after he had explained that it could not be done. Accordingly, since this type of thing happened to him often, it did not surprise CHUNG.

CHUNG did not recall CHANDRESEKARAN saying anything about his confidence in his ability to reconstruct the LIS database and he did not recall CHANDRESEKARAN saying he would later be trying to reconstruct the LIS database.

While CHUNG advised that while anything is possible, when he received this email from TAYLOR he knew it would be very difficult to reconstruct the LIS database. CHUNG was not aware of CHANDRESEKARAN having a plan to reconstruct the LIS database or of any plan in which CHANDRESEKARAN was to put the LIS database back together.

CHUNG never got a sense that there was a working copy of the LIS database somewhere.

On the last day when Theranos shut down, MCCHESNEY drove a truck with the servers and hard drives to a public storage facility. MCCHESNEY took the hard drives out of the servers to save them and took them to a different storage unit. These hard drives were the hard drives for all the production servers. The reason MCCHESNEY took the hard drives out of the servers was because he did not want to be the one who was responsible for losing this data. MCCHESNEY told CHUNG this before the servers were moved. However, once the hard drives were taken out of the servers, if they were not tracked as to where they came from, it would have been impossible to put them back together. Even if the hard drives were all labeled correctly, it would have been extremely difficult to reconstruct the database because in addition to the servers there are also hundreds of network devices which would have to be connected correctly. Accordingly, retaining these hard drives would not necessarily have meant the data on them had been retained. CHUNG was responsible for returning the servers to the lessor, and the servers did not have the hard drives in them when he returned them.

Outside of his attorneys, CHUNG has also spoken about the existence of the government investigation with his assistant, his girlfriend, ERIC CADDENHEAD (CADDENHEAD), and the Assignee for the Benefit of Creditors of Theranos (ABC). CADDENHEAD and CHUNG have a professional relationship and CADDENHEAD had hired Neetek to assist with a move at his new company. However, CHUNG has not discussed the substance of the events at Theranos with CADDENHEAD. THE ABC is aware of the investigation because they had asked CHUNG to see if Theranos' servers were still on line. On November 17, 2020 Sherwood reached out to CHUNG and asked him to see if the Theranos servers were still "healthy". They wanted CHUNG to go look at these servers, which were for the active directory which were located at the data center, and not the servers for the Laboratory Information System (LIS) database. There was also an active directory encryption mechanism which encrypts and decrypts messages. This encryption was also located at the data center which also stored the file servers and email servers. However, CHUNG thought these servers were probably "stale".

The ABC, Sherwood, and Fortress Investment Group (Fortress) wanted CHUNG to help get the Active Directory management rights running and healthy. CHUNG was not sure why they wanted him to do this, but knew that Fortress owned Theranos' Intellectual Property (IP).

EXHIBIT N

FD-302 (Rev. 5-8-10)

OFFICIAL RECORD
Document participants have digitally signed. All signatures have been verified by a certified FBI information system.

FEDERAL BUREAU OF INVESTIGATION

Date of entry 11/17/2020

MICHAEL CHUNG (CHUNG), previously interviewed, was interviewed at Hillstone Restaurant located at 1800 Montgomery Street, San Francisco, California. Also present for the interview was Assistant United States Attorney (AUSA) Vanessa Baehr-Jones. Prior to the interview, AUSA Baehr-Jones advised CHUNG it was illegal to lie to a Federal Officer (Title 18 U.S.C. 1001) and CHUNG confirmed he understood. After being advised of the identity of the interviewing parties CHUNG agreed to the interview being audio recorded.

The below is an interview summary. It is not intended to be a verbatim account and does not memorialize all statements made during the interview. Communications by the parties were electronically recorded. The recording captures the actual words spoken. A copy of the recording of the interview will be maintained in the attached 1A as well as the 1D section of the case file. Documents shown to CHUNG during the interview are also attached and will be maintained in the 1A section of the case file.

NEETEK_000576 - NEETEK_000577

CHUNG was shown NEETEK 000576 - NEETWK_000577, an email DAVID TAYLOR (TAYLOR) sent on September 2, 2018 to CHUNG, ERIC CADDENHEAD (CADDENHEAD), SHEKAR CHANDRASEKARAN (CHANDRASEKARAN), and SEKHAR VARIAM (VARIAM) titled "RE: LIS data base discussion - response to request". This email contained forwarded emails from VARIAM which were sent on August 30, 2018 and June 6, 2018.

CHUNG first recalled receiving this email forwarded from JOHN MCCHESNEY (MCCHESNEY) shortly after this email was sent. CHUNG then had to work with CADDENHEAD to find the password, and they tried to get in touch with ANTTI KORHONEN (KORHONEN) to get the password.

CHUNG interacted very little with TAYLOR.

Investigation on 10/06/2020 at San Francisco, California, United States (In Person)

File # 318A-SF-7315857 Date drafted 10/06/2020

by Mario C. Scussel

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

These were old back-ups of LIS, CHUNG did not know that they were ever able to restore these old back-ups. CHUNG advised that in IT if you have an old back-up of something you never want to assume that it is readable, you always want to try to read from it before you are comfortable that you actually have the back-up. CHUNG was not sure they were ever able to restore this old data on these USB drives.

NEETEK_000811

CHUNG was shown NEETEK 000811, an email between CHUNG and CADDENHEAD from August 8, 2018 titled "RE: Decrypted version". In the document CHUNG asks CADDENHEAD to ask KORHONEN if he can provide the password to restore the private key for the LIS database. CHUNG advised they were never able to get in touch with KORHONEN to get this password. CHUNG advised that this type of thing happened often, where CADDENHEAD would not have a password or sufficient familiarity with a system that only KORHONEN was familiar with, so CADDENHEAD would say he would reach out to KORHONEN then nothing would happen. CHUNG's job was just to tell JOHN MCCHESNEY (MCCHESNEY) that he did not get the password and he assumed MCCHESNEY would take it from there. CHUNG did not recall MCCHESNEY's exact response to this, but it was to the effect of "well if we can't get the password, then I don't know."

The LIS system was a customized, "home-grown", application, meaning one could not go out and purchase technical support for. The infrastructure the LIS lived on was a lot of infrastructure. Unlike the emails and files which could be forklifted out of the facility and into the datacenter, the LIS database could not. Even moving the emails and files from Theranos was not easy, and took months of preparation. The LIS was on completely different infrastructure consisting of hundreds of servers. Since Neetek did not know the system inside and out, the way they would know a Microsoft and VMware system, there was no way to be able to move it since it was a customized system. CADDENHEAD at least knew how to back up the LIS, so they decided to go out and purchase USB drives and back the LIS up to these USB drives. They then purchased more USB drives and backed up the LIS to those, and then CHUNG gave these USB drives to MCCHESNEY. When a system is on large infrastructure it is usually due to the system, not the size of the data in the system. Accordingly the data would be able to fit on these USB drives. If one had the data and knew how to understand it and query the data then simply having the database might be enough. However, if you want the application to be usable again by people you will have to reconstruct the whole application restore it. CHUNG did not think would not have been possible to get the LIS database to work again after it was taken apart, and thought he had told people that it could not be reconstructed as there were a lot of conversations about feasibility.

However, the password issue came up and they called SHEKAR (CHANDRASEKARAN) or someone else.

CHUNG did not go into the USB drives to look at the data, and advised he does not know about databases. CHUNG believes CADDENHEAD would have done a proper back-up.

CHUNG advised when he said he was "able to open it" this did not mean they they could open it and see the content of data.

CHUNG advised that USB drive and hard drives were the same thing in this email. It does not mean the hard drives in the database because once you take the hard drive out of the system it would be almost impossible to get it working again.

In SQL server technology in regards to encryption, just because you have made a backup you can put a password on the backup and restore the data with the password you specified, but that does not mean you know the password on the database.

CHUNG recalls there was data he was trying to open, but trying to read the contents of the data required a password which only KORHONEN had. Accordingly, CHUNG could not access the data because he did not have the password, which only KORHONEN knew.

NEETEK_000591

CHUNG was shown NEETEK 000591, an email chain from August 29, 2018 titled "RE:LIS" between CHUNG, MCCHESNEY, CHANDRASEKARAN, TAYLOR, and CADDENHEAD.

CADDENHEAD was not able to able to get authentication to connect to the server. It took CADDENHEAD several attempts to copy the LIS to the USB drives.

There were many instances when they could not get to something because of some password or unfamiliarity with the system because it was untouched for years before CHUNG started.

NEETEK_000596

CHUNG was shown NEETEK 000596, an email requesting a conference call between KATIE MORAN (MORAN), CHUNG, CHANDRASEKARAN, and CADDENHEAD. CHUNG thought this call was in regards to a conversation at the last minute where someone decided that they would have someone do a spreadsheet export to the file server, while they still had someone who could do this task. This happened hours before CHUNG shut down the LIS database. CHUNG recalls this because he had to wait for them to finish this task so he could shut down the LIS database.

CADDENHEAD had made the USB drive copy well before they did this spreadsheet export to the file server.

NEETEK_000746

CHUNG was shown NEETEK 000746, an email between CHUNG and MCCHESNEY on August 10, 2018 titled "FW: Decrypted Version". In this email CHUNG reminded MCCHESNEY that just because they made a backup of the database that does not mean that they would be able to look at this data because there was still an encryption key that they did not know. Accordingly, it did not matter how many copies they made, because they would not be able to restore the data without a key. Then the next thing CHUNG knew, CADDENHEAD was asked to make another copy, so he decided to put this warning in writing.

NEETEK_000616

CHUNG was shown NEETEK 000616, an email chain with an email from TAYLOR on August 28, 2018 which included MORAN, CHUNG, CADDENHEAD and CHANDRASEKARAN. This was the same email as on NEETEK_000596. The call referred to in this email might have been the call when they decided to put the LIS database on spreadsheets. This decision would have been made by either TAYLOR or MCCHESNEY.

CHUNG advised that a SQL database could be translated into Excel, but only if the data could be limited to rows and columns. However, if one needed more than rows and columns, a more three dimensional view, then one would need a more powerful system than Excel. CHUNG did not recall a discussion on the call of whether the data would work in Excel. Either TAYLOR or MCCHESNEY would have been the one who made the decision to put the data on Excel spreadsheets. CHUNG did not have that level of involvement in the business, as his team was more hired as a forklift operator for IT stuff. While he knows a lot about this type of thing, CHUNG stayed in his lane in his business. CHUNG vividly recalled having to wait for the guy to finish downloading spreadsheets in order to shut down the LIS.

CHANDRASEKARAN knew very little, he was just someone who had worked on the LIS system a long time ago.

It was clear during this conversation that they were never able to get the encryption key and CHUNG recalled telling MCCHESNEY that they were not able to decrypt the data.

CHUNG did not speak with TAYLOR and KATIE MORAN (MORAN) in detail as they were several levels above him. Most of CHUNG's communication was with MCCHESNEY and CADDENHEAD.

NEETEK_000580

CHUNG was shown NEETEK 000580, an email from September 2, 2018 titled "RE: Info for Shekar" between CHUNG, TAYLOR, and CADDENHEAD. This email implies that TAYLOR wanted to rebuild the LIS database because four things TAYLOR was asking for were the things necessary to rebuild the database. If anyone were to ask CHUNG for these things it would imply that they were trying to build the system again. It was strange that TAYLOR would be asking to rebuild the LIS database just days after taking it apart, and just days after reminding everyone it would be hard to resuscitate the database after taking it apart.

CHUNG advised that the Theranos project was very annoying for Neetek, as either a system would simply not be working or they constantly did not have passwords that they needed. There was not a lot of time pressure as they had months to prepare. The only time pressure in the project was getting email and files up and running at the co-location by Monday morning, which they were able to do.

NEETEK_000334 to NEETEK_000335

CHUNG was shown NEETEK 000334 to NEETEK_000335, an email chain from MORAN on August 29, 2018 titled "RE: Call re LIS (priv/conf) - time sensitive in which MORAN asks CADDDENHEAD if he was able to pull a copy of the LIS software from the share drive. CHUNG, CHANDRESEKARAN, and TAYLOR are also copied on this email which was the day after they had a conference call.

Later in the chain on September 14, 2018 MORAN emails CADDENHEAD asking him to copy the code for the LIS onto a hard drive.

CHUNG thinks MORAN was looking for the binaries here, which would have been the application files, not the database files. This would have given her two of the four things necessary to rebuild the LIS database. LIS software code would include the source code. The four things necessary to try to rebuild the LIS database would have been the encryption keys, binary, database, and the build production documents.

It would have been a gargantuan effort to rebuild this system from scratch. However, they would need the encryption key, so it would be impossible to rebuild it without this, and they did not have it. Even if they had everything to include the encryption key it would take a team of engineers and project managers to put the LIS database back together. Regardless, they would need to have the private key, no matter what.

The LIS system was functional all summer and the guy who downloaded the spreadsheets was able to access the system. CHUNG did not recall this person's name, but he was one of only about ten people left at the company at the end. CHUNG was not sure why this person was not included on these emails at the end. CHUNG thought MCCHESNEY would know who this person was because MCCHESNEY would have been the person who told him to download the spreadsheets. This person told MCCHESNEY that he was done downloading, and then MCCHESNEY would have told CHUNG that he could go ahead and shutdown the LIS database.

The database had a password that CHUNG did not have, while one can open the database if they have the right software, one cannot get to data without the key.

EXHIBIT O

FD-302 (Rev. 5-8-10)

OFFICIAL RECORD

FEDERAL BUREAU OF INVESTIGATION

Date of entry 01/08/2021

JAROD WADA (WADA) was interviewed via video teleconference. Representing WADA during the interview were Stephen O'Neill and Caitlin Hull from Dorsey & Whitney (Dorsey). Also present for the interview were Assistant united States Attorney (AUSA) Vanessa Baehr-Jones and AUSA Bob Leach. Prior to the interview AUSA Baehr-Jones reminded WADA that it is illegal to lie to a Federal Officer (Title 18 U.S.C. 1001). After being advised of the identity of the interviewing parties and the nature of the interview, WADA provided the following information:

WADA has been a Senior Vice President at Sherwood Partners (Sherwood) for the past two and a half years. Prior to working at Sherwood Partners Wada amassed 20 years of experience in business advisory services for distressed businesses working for PricewaterhouseCoopers (PWC) and FTI Consulting (FTI). WADA left FTI in January 2018. In his role at Sherwood, WADA's day to day role for their client Theranos included being the primary contact person for temporary employees, creditors, vendors, custodians for corporate documents, and the lender. The lender in this case was Fortress Investment Group (Fortress).

An Assignment for the Benefit of Creditors (ABC) was an insolvency process similar to filing Chapter 7 or 11 Bankruptcy. The ABC handles all assets and attempts to monetize those assets to the best of their ability. The ABC also validates claims from creditors and makes distributions. Sherwood was hired for a pre-ABC diligence task by Theranos in the last week of July and beginning of August 2018. In performing this task, Sherwood was looking at who Theranos' creditors were, how much they were owed, and other tasks to determine if Sherwood was willing to be the ABC for Theranos. Sherwood was also determining how much their fees would be to be the ABC for Theranos.

Litigation requests were handled mostly through Dorsey and Wilmer Hale.

Investigation on 12/17/2020 at San Francisco, California, United States (Phone, Other (Video teleconference))

File # 318A-SF-7315857 Date drafted 12/17/2020

by Mario C. Scussel

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

During the pre-ABC process Sherwood did some work to figure out where these legal matters stood in order to assess the budget they would need to retain Dorsey.

WADA did not specifically recall getting into the legal requests. Sherwood was assessing the situation in order to prepare for where these documents might go as they had to know where documents were and how to get them. Sherwood also needed to know this information to know who they would need to hire.

WADA did not have any specific recall of the Laboratory Information System (LIS) database from this time. WADA knew of the existence of the LIS database, and confirmed that copies of it had been made and had been delivered to people at this point. However, WADA did not recall who had received the copies of the LIS database at that time. After Sherwood had been hired as the ABC, Dorsey had delivered a copy of the LIS database to the plaintiff attorney in the Arizona litigation.

PWC had been previously been engaged by Wilmer Hale, and they turned over a copy of an e-discovery database containing documents from Theranos which could be queried.

WADA was shown a chain of emails bates stamped TheranosABC00002013 - TheranosABC00002019. In the email WADA mentions discussions with PWC regarding encryption. Theranos had set up an Information Rights Management System (IRM) which would encrypt any document stored on Theranos' corporate servers. In order to provide documents to PWC, they had to run the IRM in order to decrypt them. WADA never had discussions with PWC as to whether they had access to the LIS database. However, WADA did know that FTI had access to the LIS database as part of their litigation support.

SHEKAR CHANDRASEKARAN's (CHANDRASEKARAN) name came up after Sherwood had been hired as the ABC for Theranos. WADA was not aware of CHANDRASEKARAN prior to the start of the assignment. CHANDRASEKARAN's name came up during the Arizona litigation because the counsel could not open the copy of the LIS database they have been given. WADA was not sure if CHANDRASEKARAN was a contractor or a Theranos employee. CHANDRASEKARAN's name also came up when Fortress was asking for people who were on a list of people regarding Intellectual Property (IP).

The ABC did look at the amount of money that had been paid out to vendors, but WADA could not recall exactly how much had been paid to IncRev Corporation. While WADA could not recall the amount he knew there was a report completed for how much had been paid to vendors for the year prior. The ABC was not in a position to know if Theranos paid someone too much or too little. Instead they were looking for payments to insiders or if certain vendors might have been given preferential treatment. WADA did not recall and findings in regards to IncRev Corporation.

WADA had seen contractor agreements for IncRev for an on-shore and an off-shore software development team. The assignee would only be looking to see if they had been paid in accordance with their contract.

Sherwood first learned that copies of the LIS database were not accessible after assignment. They learned this right at assignment which was on September 12, 2018. Sherwood knew they had been encrypted. This became and issue when it was provided to the Plaintiff's counsel in the Arizona litigation and they could not access it. This is when it rose to the ABC's level and they started asking questions and reaching out to people to include ERIC CADDENHEAD (CADDENEHAD). Sherwood then learned that FTI had been involved so WADA reached out to MIKE WEI (WEI) at FTI. From FTI, Sherwood learned that a copy of the LIS database had been made, but was stored on Theranos' corporate database so FTI could run reports. The reports run by FTI were mostly in regards to the Arizona Attorney General's settlement. WEI checked to see if the LIS database could still be accessed. While the remote access still seemed to exist the LIS database was not still there.

FTI had a report of the amount of money patients had spent at Theranos, and this was the report which was used for the settlement in the Arizona Attorney General's litigation. This was the report they needed so once they found this report the ABC did not continue to try to get into the LIS database.

Sherwood first learned that the LIS database was encrypted from KATIE MORAN (MORAN) at Wilmer Hale and DAVID TAYLOR (TAYLOR) at Theranos. There was only a small group at Theranos who knew that the company was considering an ABC.

The ABC had limited people to contact to try to get answers when they learned the United States Attorney's Office was trying to access the LIS database. The people they could contact included: CADDENHEAD, TAYLOR, WEI, and MICHAEL CHUNG (CHUNG) from Neetek. When they asked people how to get into the LIS database, CHANDRASEKARAN's name came up. However, WADA never got in touch with CHANDRASEKARAN. CADDENHEAD explained that the answer, as to the best of his understanding, of the LIS database fell outside of Theranos employees as it was not internal Theranos IT people who built the LIS. Instead it would have been CHANDRASEKARAN who they would need to contact.

When the LIS database question came up, TAYLOR also reached out to BRAD ARRINGTON and KING DAS.

Neetek was responsible for moving servers to a co-location in Sunnyvale, California.

WADA was shown a chain of emails from September and October 2018 bates stamped DTTPROD-000000146 to DTTPROD-000000151. WADA recalled these emails and explained that when companies have leased equipment they are not going to continue paying, but instead will surrender the equipment as long as the equipment was not a media storage device. Accordingly they could return the server but not the hard drives/data the servers contained. This was an ongoing surrender of equipment and the lessor was trying to schedule a time to pick up the equipment. Neetek attempted to locate the equipment in the co-location and a public storage locker using serial numbers, and they segregated this equipment. WADA did not know if these were the LIS servers that they were returning to the lessor or if they were other servers. WADA's understanding from CADDENHEAD was that Theranos was going to transition to new servers and these were those new servers which Theranos was going to transition to. The servers that were up and running at the co-location were Theranos' email servers and share drives, but not the LIS database. The equipment for the LIS database might have been in the public storage locker, but WADA understood the data had been taken out and copied. There were three public storage lockers, one which contained proprietary lab equipment and another that had non-proprietary lab equipment. There was never an inventory of what was in these storage lockers. WADA was the only person who was authorized to access these lockers.

WADA advised that Wilmer Hale had been requested to provide them with everything which would have included any information regarding and encryption password for the LIS database.

Sherwood also hired ANTTI KORHONEN (KORHONEN) as a limited scope temporary employee to assist with the IRM system. Both KORHONEN and CADDENHEAD were asked and neither of them were involved in the encryption or decommissioning of the LIS database.

WADA never followed up with Davis, Wright, & Termaine (DWT) about CHANDRASEKARAN. Dorsey was unclear if they ever provided a hard drive copy of the LIS to DWT.

Documents shown to WADA during the interview are attached and will be maintained in the 1A section of the case file.

EXHIBIT P

From: Jarod Wada <[redacted]>
To: Michael Chung <[redacted]>
Cc: David Taylor <[redacted]>, "philippepoux[redacted]>
Subject: Theranos ABC - Cisco capital lease equipment
Sent: Fri, 12 Oct 2018 15:42:22 +0000

Michael,

Based upon our various discussions on this equipment, the following will be our approach.

1. Neetek will hold until the lessor/lessor's servicing company reaches back out to me again demanding either the buyout payment or surrender of equipment.
2. When I receive that request, I will authorize Neetek to take on the task of sorting through the IT Equipment locker to segregate the relevant equipment, however, we will also need to sort out those pieces of equipment that contain hard drives vs. those that do not.
3. I will then work out with the lessor that we can only voluntary surrender the equipment that does not have stored media / data due to the hold resulting from pending litigation (will mention the DOJ).
4. Then proceed from there based upon the Lessor's reaction.

Thank you.

Regards,
Jarod

SHERWOOD Partners, Inc.
Solutions | Results | Success | Since 1992

Jarod J. Wada
jwada@[redacted]
[redacted] Direct
www.shrwood.com

Silicon Valley | Los Angeles | New York

CONFIDENTIALITY NOTICE: This e-mail transmission, and any documents, files or previous e-mail messages attached to it, may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this message is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify us by reply e-mail at info@shrwood.com or by telephone at (650) 454.8030, and destroy the original transmission and its attachments without reading them or saving them to disk. Thank you.
IRS CIRCULAR 230 DISCLOSURE: To comply with requirements imposed by recently issued treasury regulations, we inform you that any U.S. tax advice contained in this communication (including any attachments) is not intended or written by us, and cannot be used by you, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another person any transaction or matter addressed herein.